STORAGE – Jurnal Ilmiah Teknik dan Ilmu Komputer, Vol. 5 No. 3, Agustus 2026, 362 – 372
e-ISSN: 2828-5344 | DOI: 10.55123

Implementasi Intrusion Prevention System Berbasis Variational Autoencoder untuk Mencegah Judi Online pada Jaringan Komunitas

[1)]Aan Alma Khanafi [2)] Indra Lina Putra [3)] Tutik Khotimah
[1,2,3)]Teknik Informatika, Teknik, Universitas Muria Kudus
[1)]aanalma03@gmail.com, [2)]indra.putra@umk.ac.id [3)]tutik.khotimah@umk.ac.id

INFO ARTIKEL

Riwayat Artikel :
Diterima : 29 Juni 2026
Disetujui : 10 Agustus 2026

Kata Kunci :
Variational Autoencoder, *Deep Neural Network, Intrusion Prevention System*, Judi *Online,* Keamanan Jaringan, *Encrypted Traffic Classification,* Deteksi Anomali, API Mikrotik

ABSTRAK

Fenomena perjudian online menimbulkan dampak negatif yang masif di Indonesia, baik secara finansial maupun psikologis. Penelitian ini bertujuan untuk mengembangkan IPS (*Intrusion Prevention System*) berbasis pembelajaran mesin guna melakukan aksi pencegahan secara preventif terhadap pengguna jaringan yang mengakses situs judi online, termasuk yang menggunakan teknik penyembunyian terenkripsi. Penelitian ini menggunakan metode kuantitatif eksperimental dengan memanipulasi variabel fitur pada dataset serta mengoptimalkan arsitektur VAE (*Variational Autoencoder*) dan DNN (*Deep Neural Network*). Hasil penelitian menunjukkan bahwa model VAE mampu melakukan rekonstruksi data dan mengelompokkan trafik judi online dengan trafik normal secara presisi, yang dibuktikan melalui visualisasi plot t-SNE. Pada tahap klasifikasi, model DNN mencapai akurasi keseluruhan sebesar 80,80%. Evaluasi spesifik per skenario menunjukkan rata-rata akurasi sebesar 95,13% untuk label judi *online* (presisi 0,69, recall 0,91, F1-score 0,78) dan 87,69% untuk label normal (presisi 0,93, recall 0,75, F1-score 0,83). Sistem pemantauan trafik yang dikembangkan juga telah terintegrasi dengan router MikroTik melalui API, sehingga fungsi pemblokiran otomatis pada level jaringan dapat beroperasi dengan baik.

ARTICLE INFO

Article History :
Received : Jun 29, 2026
Accepted : Aug 10, 2026

Keywords*:*
Variational Autoencoder, Deep Neural Network, Intrusion Prevention System, Online Gambling, Network Security, Encrypted Traffic Classification, Anomaly Detection, Mikrotik API.

ABSTRACT

The phenomenon of online gambling causes massive negative impacts in Indonesia, both financially and psychologically. This study aims to develop a machine learning-based IPS (Intrusion Prevention System) for preventive actions against network users accessing online gambling sites, including those employing encrypted hiding techniques. This research applies an experimental quantitative method by manipulating feature variables in the dataset and optimizing the architecture of the VAE (Variational Autoencoder) and DNN (Deep Neural Network). The results indicate that the VAE model successfully reconstructed the data and accurately clustered online gambling traffic from normal traffic, as evidenced by the t-SNE plot visualization. In the classification stage, the DNN model achieved an overall accuracy of 80.80%. Specific evaluations per scenario indicated an average accuracy of 95.13% for the online gambling label (precision 0.69, recall 0.91, F1-score 0.78) and 87.69% for the normal label (precision 0.93, recall 0.75, F1-score 0.83). The developed traffic monitoring system has also been successfully integrated with the MikroTik router via API, ensuring the automatic blocking function at the network level operates effectively..

1. PENDAHULUAN

Fenomena judi online di Indonesia menimbulkan dampak kerugian finansial dan psikologis masif yang mendesak pemerintah melakukan pemblokiran situs secara agresif (Mayradevi and Tobing, 2024; Gu et al., 2024; Antonio et al., 2025). Namun, para pemain kerap menghindari pembatasan tersebut menggunakan teknik penyembunyian aktivitas jaringan seperti VPN, DoH, dan DoT yang mengenkripsi resolusi DNS, sehingga menyulitkan pemantauan aktivitas jaringan secara konvensional (Monroy et al., 2023; Alkasassbeh Mouhammd and Almseidin, 2023; Alzighaibi, 2023; Guerra-Manzanares et al., 2025).

Sistem keamanan jaringan konvensional seperti IDS (*Intrusion Detection System*) dengan metode DPI (*Deep Packet Inspection*) berbasis tanda tangan (*signature-based*) memang mampu mengidentifikasi tujuan domain (Azam et al., 2023; Abuajwa et al., 2025). Namun, metode ini membutuhkan sumber daya yang besar, dapat memperlambat jaringan internet (Syafi'i Bachtiar et al., 2024), dan kurang efektif dalam mendeteksi aktivitas trafik tersandi yang tanda tangannya belum terdaftar di daftar hitam (Sari et al., 2024). Oleh karena itu, pendekatan keamanan saat ini mulai bergeser menuju sistem *anomaly-based* menggunakan pembelajaran mesin agar lebih akurat dalam mendeteksi trafik terenkripsi (Laghrissi et al., 2021; Alwhbi et al., 2024). Terkait hal ini, penelitian (Rahayu Prasiska, 2025) telah berhasil mengklasifikasikan trafik judi online menggunakan kombinasi *Autoencoder* dan DNN (*Deep Neural Network*) dengan akurasi 99,87%, namun penelitian tersebut belum menguji performa model terhadap trafik jaringan yang disembunyikan. Di sisi lain, penelitian (Monroy et al., 2023) membuktikan efektivitas *Autoencoder* dalam mendeteksi anomali pada trafik DoH secara spesifik, meskipun fokus ancamannya adalah serangan siber *Zero-Day*, bukan pada perilaku akses judi online.

Beberapa literatur terdahulu telah mengeksplorasi penggunaan kecerdasan buatan dalam deteksi lalu lintas jaringan. Hasin et al. (2023) memanfaatkan *framework* NFStream dan TensorFlow untuk mendeteksi serangan DDoS berbasis HTTP. Dalam ranah klasifikasi lalu lintas terenkripsi, Yang et al. (2025) berfokus pada deteksi terowongan DoH berbahaya, sementara Correia et al. (2025) membuktikan keandalan VAE (*Variational Autoencoder*) untuk mendeteksi anomali pada data deret waktu diskrit. Meskipun pendekatan *Anomaly-Based Intrusion Detection System* (Vasudev et al., 2025) telah terbukti lebih unggul daripada sistem berbasis *signature* tradisional, mayoritas penelitian tersebut masih berfokus pada serangan siber konvensional dan belum menyentuh deteksi aktivitas perjudian online yang disamarkan menggunakan VPN (Karuna Jyothi and Reddy, 2023).

Tabel 1 Perbandingan Penelitian Terkait

Peneliti	Fokus Deteksi	Algoritma	Kelemahan
Hasin et al. (2023)	Serangan HTTP DDoS	NFStream, Tensorflow	Hanya berfokus pada trafik HTTP, gagal pada trafik terenkripsi
Yang et al. (2025)	Terowongan DoH (*Malicious*)	Machine Learning	Tidak dievaluasi menggunakan protokol penyamaran lain.
Correia et al. (2025)	Anomali Deret Waktu	Variational Autoencoder	Tidak diimplementasikan sebagai sistem pencegahan (IPS) secara *near real-time*.

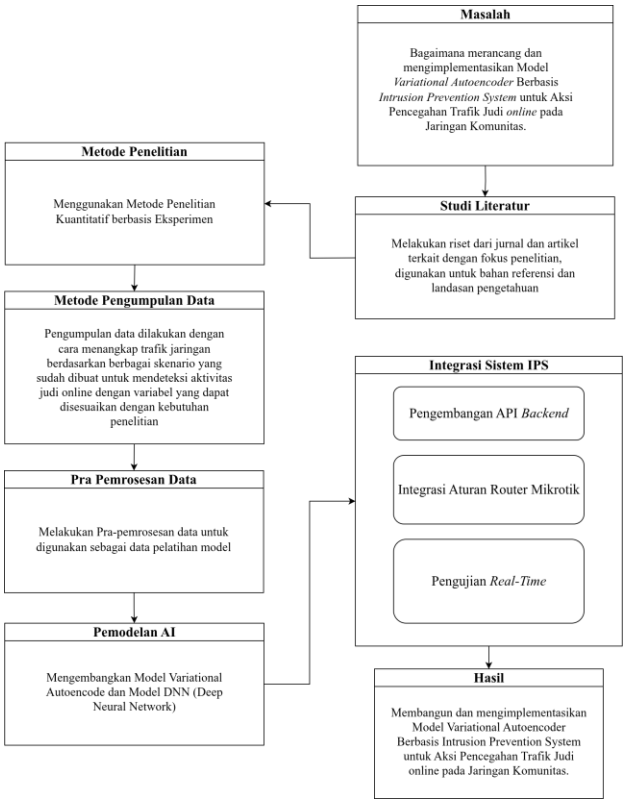
Berdasarkan celah penelitian pada Tabel 1, penelitian ini mengusulkan tiga kontribusi kebaruan:

1. Penggunaan ekstraksi fitur statistik non-*payload* berbasis *Inter-Arrival Time* (IAT) menggunakan NFStream untuk mengklasifikasi trafik judi online yang disamarkan oleh VPN, DoH, dan DoT.
2. Implementasi arsitektur hibrida VAE untuk mereduksi *noise* (Scourfield et al., 2023) yang digabungkan dengan DNN (Domínguez-Morales et al., 2024; Eman Jawad, 2023) sebagai pengklasifikasi akhir.
3. Integrasi agen pemantauan berkelanjutan yang mengeksekusi pemblokiran secara *near real-time* langsung pada *router* MikroTik bermemori rendah melalui komunikasi API.

2. METODE

2.1. Desain Penelitian dan Spesifikasi Perangkat

Penelitian ini menggunakan pendekatan kuantitatif berbasis eksperimental. Fokus utama metode ini terletak pada alur kerja pembelajaran mesin (*machine learning pipeline*) yang mencakup pengumpulan lalu lintas jaringan, rekayasa fitur, pra-pemrosesan, pemodelan VAE-DNN, hingga integrasi otomatis dengan *router*. Metode *Waterfall* juga digunakan, namun peranannya dibatasi hanya sebagai panduan siklus hidup dalam pengembangan aplikasi antarmuka web pemantauan. Pendekatan eksperimental digunakan agar variabel penelitian, seperti fitur *dataset* dan *hyperparameter* arsitektur kecerdasan buatan, dapat dimanipulasi secara leluasa untuk memaksimalkan hasil akurasi. Alur kerja sistem secara keseluruhan dapat dilihat pada Gambar 1.

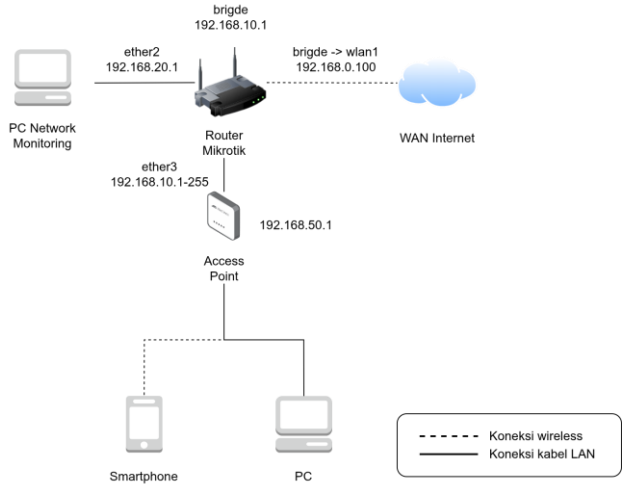


Gambar 1 Alur Kerangka Kerja Penelitian

Spesifikasi perangkat keras yang digunakan meliputi PC Server (Asus X455LF, Intel Core i3 1.70 GHz, RAM 10GB dengan lingkungan CPU 4-*thread*) untuk menangani komputasi AI. Infrastruktur jaringan menggunakan Router MikroTik RB941-2nD (CPU 650 MHz, RAM 32MB). Pemilihan MikroTik seri ini didasarkan pada alasan kepraktisan, harganya yang terjangkau, dan sangat umum digunakan pada konfigurasi jaringan komunitas (RT/RW Net). Mengingat kapasitas RAM 32MB menjadi keterbatasan utama untuk pemrosesan kecerdasan buatan secara langsung, proses inferensi (*inference*) model AI diisolasi secara khusus pada PC Server, sementara router murni difungsikan untuk eksekusi port mirroring dan API. Selain itu, digunakan pula Access Point TP-Link TL-WR840N untuk melayani perangkat klien nirkabel. Perangkat lunak dikembangkan menggunakan bahasa Python dalam lingkungan Docker, memanfaatkan kerangka kerja NFStream untuk ekstraksi fitur paket secara mendalam..

2.2. Teknik Pengumpulan Data

Trafik klien direkam secara spesifik dengan mengunjungi 15 situs web judi *online* yang berbeda beserta berbagai variasi situs web normal. Proses perekaman lalu lintas (*sniffing*) dilakukan dengan durasi sekitar 15 hingga 30 menit untuk setiap bagian (*part*) sesi pada masing-masing skenario penyamaran (Akses Normal, VPN, DoH, dan DoT). Trafik mentah direkam ke dalam format PCAP (*Packet Capture*) dan diekstraksi menggunakan *framework* NFStream menjadi format CSV. Guna mencegah terjadinya kebocoran data (*data leakage*), *dataset* tidak dibagi secara acak (*random split*). Pemisahan data dilakukan secara kronologis (*chronological split / forward-chaining*) berurutan waktu untuk setiap kategori pelabelan. Sebanyak 80% aliran data (*network flow*) dari sesi awal digunakan sebagai data latih, dan 20% sisa sesi akhir murni dialokasikan sebagai data uji. Pendekatan ini memastikan bahwa model selalu dievaluasi menggunakan rentang waktu data masa depan yang belum pernah dilihat sebelumnya. Topologi jaringan pengumpulan data dapat dilihat pada Gambar 2.



Gambar 2 Topologi Pengumpulan Data

2.3. Pra-pemrosesan Data

Tahap pra-pemrosesan diawali dengan ekstraksi dan seleksi fitur yang difokuskan pada IAT (*Inter-Arrival Time*) dan statistik volumetrik, mengingat fitur-fitur non-*payload* tersebut tidak dapat dimanipulasi secara penuh oleh teknik penyamaran enkripsi. Proses ini menghasilkan 26 fitur final yang digunakan sebagai masukan model. Fitur tersebut mencakup atribut temporal dan volumetrik dasar (durasi, *bytes*, paket dua arah), statistik ukuran paket (Min, Max, Mean, Std Dev), statistik IAT, hingga variabel turunan hasil rekayasa fitur seperti *payload ratio*, kepadatan paket (*packet density*), dan rasio ukuran paket (*tiny, small, medium, large*). Selain itu, terdapat pula fitur kategori yang direpresentasikan dalam format *One-Hot Encoding* untuk mendeskripsikan protokol (TCP/UDP) dan *port* tujuan (seperti 53, 80, 443, dan 853). Detail fitur dapat dilihat pada Tabel 2.

Tabel 2 Daftar 26 Fitur Input Model VAE

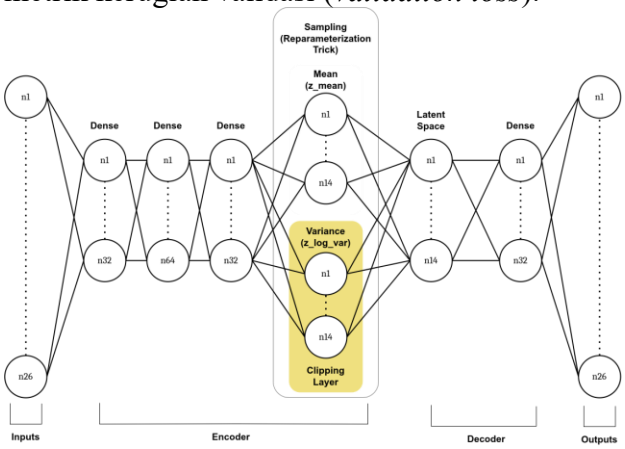
Kelompok Fitur	Nama Atribut / Fitur	Deskripsi dan Kegunaan
Atribut Temporal & Volumetrik Dasar	bidirectional_duration_ms, bidirectional_packets, bidirectional_bytes	Mengukur durasi total aliran (*flow*), jumlah total paket dua arah, dan volume data yang dipertukarkan.
Statistik Ukuran Paket	bidirectional_min_ps, bidirectional_max_ps, bidirectional_mean_ps, bidirectional_stddev_ps	Menangkap nilai minimum, maksimum, rata-rata, dan standar deviasi dari ukuran paket untuk mendeteksi keseragaman muatan.
Statistik Jeda Waktu (*IAT*)	bidirectional_min_piat_ms, bidirectional_mean_piat_ms, bidirectional_stddev_piat_ms	Mengukur jeda waktu antar-kedatangan paket (*Inter-Arrival Time*) untuk mengidentifikasi pola ritme komunikasi.
Fitur Turunan (*Derived Features*)	Payload_ratio, packet_density, download_upload_ratio	Variabel rekayasa untuk melihat rasio muatan terhadap header, kepadatan aliran paket per detik, serta keseimbangan trafik unduh-unggah.

Rasio Ukuran Paket	ps_tiny_ratio, ps_small_ratio, ps_medium_ratio, ps_large_ratio	Proporsi klasifikasi ukuran paket ke dalam kategori kecil (*tiny/small*) hingga besar (*medium/large*).
Atribut Kategorikal (*One-Hot Encoded*)	protocol (TCP/UDP), dst_port (53, 80, 443, 853)	Identifikasi protokol transport dan port tujuan utama (termasuk port DNS, HTTP, HTTPS, dan DoT/DoH).

Untuk mengoptimalkan sebaran data, distribusi statistik jaringan yang memiliki kemiringan ekstrem dinormalisasi menggunakan transformasi logaritmik (Log1p), serta digabungkan dengan metode *RobustScaler* untuk membatasi nilai *outlier* berdasarkan rentang interkuartil. Data target juga dipetakan menjadi format biner (0 untuk normal, 1 untuk anomali) melalui proses *Label Encoding*.

2.4. Pemodelan Kecerdasan Buatan dan Analisis Data

Teknik analisis data dirancang menggunakan arsitektur *deep learning* dan *variational autoencoder* yang divisualisasikan pada Gambar 3. Model VAE (*Variational Autoencoder*) dirancang sebagai ekstraktor fitur yang memetakan input statistik ke dalam distribusi ruang laten berdimensi 14. Proses pemetaan ini dioptimalkan menggunakan fungsi kerugian divergensi *Kullback-Leibler Divergence* untuk menjaga keteraturan ruang laten. Representasi laten tersebut kemudian diteruskan ke DNN (*Deep Neural Network*) untuk proses klasifikasi. Arsitektur DNN dirancang dengan empat lapisan tersembunyi yang masing-masing berkapasitas 128, 64, 32, dan 16 *node*, serta dilengkapi lapisan *Dropout* dan fungsi aktivasi ReLU. Untuk menangani ketidakseimbangan proporsi data, proses pelatihan menerapkan fungsi *compute_class_weight* yang memberikan penalti lebih besar pada kelas minoritas. Pelatihan model diatur menggunakan ukuran angkatan (*Batch Size*) sebesar 32 dan batas maksimum 150 *Epoch*. Pembaruan bobot jaringan dieksekusi menggunakan pengoptimal Adam dengan *Learning Rate* bawaan (0,001). Guna mencegah indikasi *overfitting*, mekanisme *Early Stopping* diterapkan dengan parameter *patience* sebesar 12, yang terbukti secara otomatis menghentikan proses pelatihan pada *epoch* ke-69 ketika tidak ditemukan lagi perbaikan yang signifikan pada metrik kerugian validasi (*validation loss*).



Gambar 3 Arsitektur Variational Autoencoder

2.5. Pengembangan dan Pengujian Antarmuka Sistem

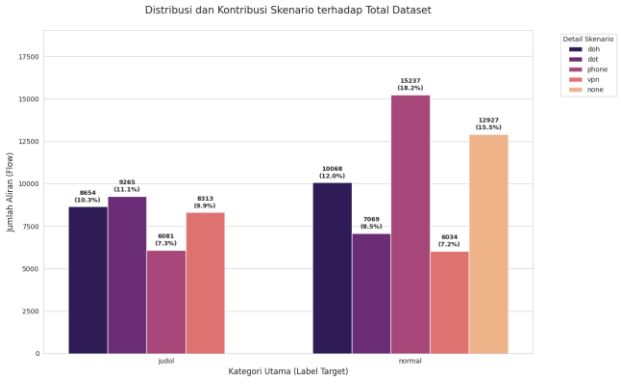
Untuk memfasilitasi pemantauan jaringan secara *real-time*, arsitektur sistem ini dilengkapi dengan antarmuka berbasis web. Sisi *backend* dikembangkan menggunakan kerangka kerja Flask Python yang bertugas mengelola aliran data dari agen AI, mencatat riwayat ke *database* SQLite, dan menjembatani komunikasi API *(Application Programming Interface*) dengan *router* MikroTik. Sisi antarmuka dibangun menggunakan kerangka kerja Svelte untuk menyajikan visualisasi data yang responsif. Komunikasi dua arah antara peladen dan klien web difasilitasi oleh protokol *WebSocket* dengan pustaka SocketIO. Pengujian kelayakan web ini menggunakan metode *Blackbox Testing* untuk memvalidasi fungsionalitas navigasi, sinkronisasi *database*, serta kecepatan pembaruan log pencegahan.

3. HASIL DAN PEMBAHASAN

3.1. Hasil Ekstraksi dan Pra-pemrosesan Data Jaringan

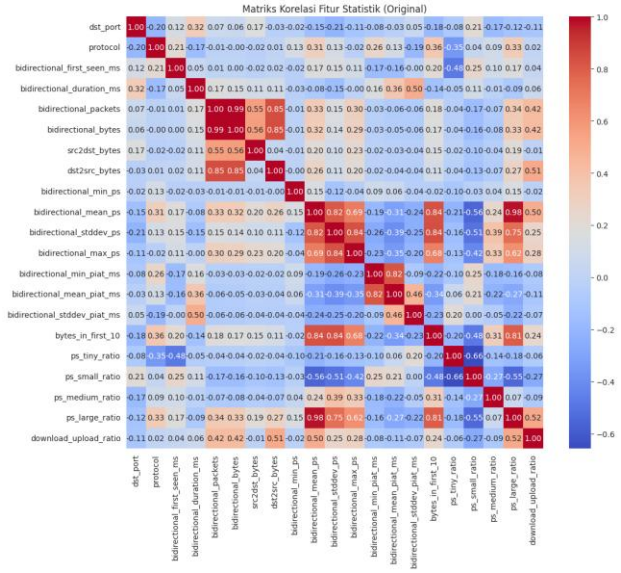
Proses pengumpulan aliran data menghasilkan dataset primer sebanyak 83.648 data. Analisis proporsi kelas target berdasarkan variasi skenario (VPN, DoH, DoT, Ponsel, dan Akses Normal) membuktikan bahwa dataset

terdistribusi dengan cukup seimbang dan tidak memiliki bias kelas yang sangat ekstrem. Diagram batang pada Gambar 4 secara visual memperlihatkan bahwa setiap skenario penyamaran memberikan kontribusi data yang proporsional, di mana kelas judi *online* dan kelas normal sama-sama terwakili secara komprehensif, sehingga mencegah model mengalami kecenderungan memihak pada satu kelas tertentu.



Gambar 4 Distribusi Frekuensi Label Kategori Dataset

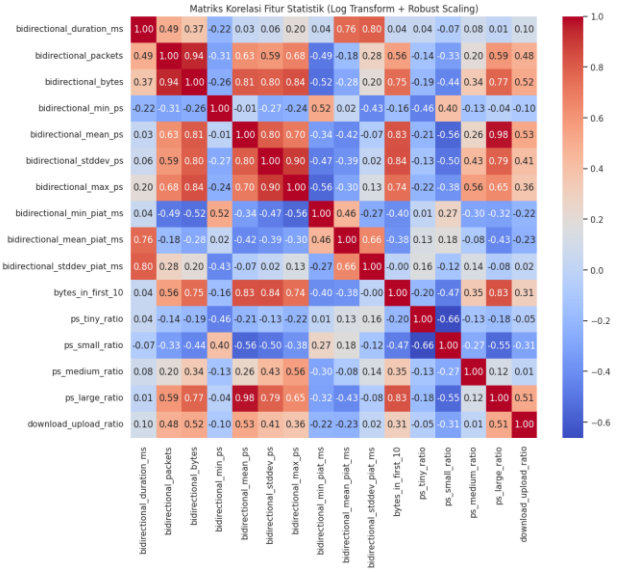
Analisis Data Eksploratif terhadap fitur-fitur jaringan menunjukkan adanya redundansi dan ketimpangan yang sangat tinggi. Visualisasi matriks korelasi pada Gambar 5 memperlihatkan peta panas dengan warna pekat pada kelompok fitur volumetrik, seperti hubungan antara jumlah paket dua arah (*bidirectional_packets*) dengan jumlah paket sumber ke tujuan (*src2dst_packets*). Hal ini menandakan adanya ketergantungan linear yang sangat kuat antar-fitur berbasis volume.



Gambar 5 Matriks Korelasi Fitur Statstik Original

3.2. Hasil Pra-pemrosesan Data

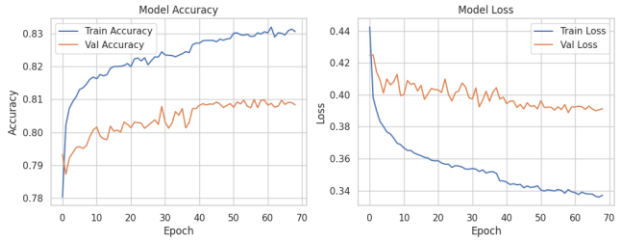
Hasil dari pra-pemrosesan ini terlihat jelas pada matriks korelasi baru di Gambar 6. Peta panas menunjukkan hubungan antar-fitur temporal dan volumetrik yang jauh lebih terstruktur dengan variasi nilai korelasi yang lebih moderat. Berkat stabilisasi ini, sebaran distribusi fitur temporal seperti rata-rata jeda waktu (*Inter-Arrival Time*) menjadi jauh lebih teratur dan representatif, sehingga secara efektif mencegah penumpukan nilai ekstrem yang dapat mendistorsi proses ekstraksi fitur pada ruang laten model.



Gambar 6 Matriks Korelasi Fitur Statistik Setelah Pra-pemrosesan

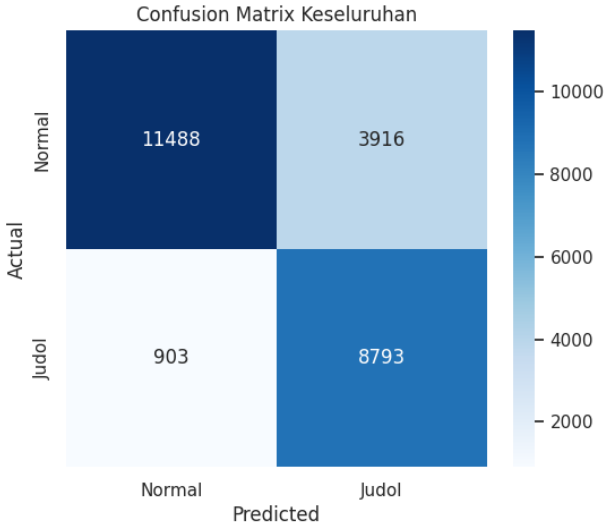
3.3. Hasil Pelatihan dan Evaluasi Model Kecercasan Buatan

Model VAE (*Variational Autoencoder*) berhasil mengompresi data ke dalam ruang laten 14 dimensi dengan *Loss* akhir 3,9390. Klasifikasi lanjutan menggunakan DNN (*Deep Neural Network*) mencapai konvergensi dan dihentikan otomatis dengan *early stopping* pada *epoch* ke-69. Grafik pergerakan akurasi dan kerugian pada Gambar 7 memperlihatkan garis *Training* dan *Validation* yang masih memiliki *gap* yang cukup jauh namun stabil, membuktikan bahwa model mempelajari pola data validasi dengan kurang baik dan tidak terjadi *overfitting*.



Gambar 7 Grafik Akurasi dan Loss pada Pelatihan Model DNN

Pengujian menggunakan 25.100 data uji memvalidasi ketajaman model. *Confusion Matrix* pada Gambar 8 secara transparan memperlihatkan model berhasil menebak 8.793 data True Positive (judi *online*) dan 11.488 True Negative (normal), dengan angka kegagalan deteksi (False Negative) yang tertekan di angka 903. Tabel 3 meringkas metrik evaluasi tersebut, menghasilkan *Recall* sebesar 0,91 dan *F1-Score* 0,78 untuk pendeteksian judi online.



Gambar 8 Confusion Matrix pada Keseluruhan Testing Set

Tabel 3 Laporan Hasil Klasifikasi Model

Kategori	***Precision***	**Recall**	**F1-Score**	**Support**
Normal	0,93	0,75	0,83	15.404
Judol	0,69	0,91	0,78	9.696
Rata-Rata	**0,81**	**0,83**	**0,81**	**25.100**

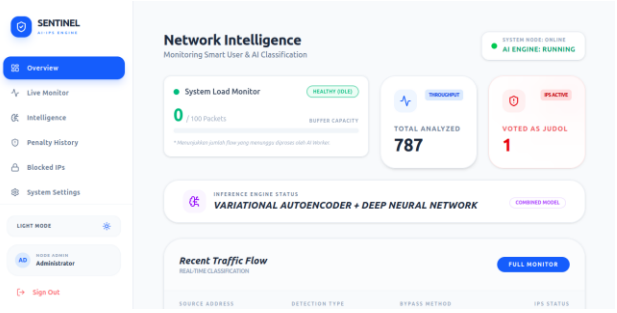
Evaluasi mendalam menggunakan metrik klasifikasi standar (Vujovic, 2021) menunjukkan adanya anomali performa pada skenario "VPN Normal", yang memicu tingginya angka *False Positive* hingga mencapai 3.916 aliran data. Kondisi ini secara rasional disebabkan oleh karakteristik enkripsi VPN yang melakukan enkapsulasi terhadap seluruh muatan paket (*payload*). Ketika pengguna melakukan aktivitas normal yang memakan *bandwidth* besar seperti pengunduhan latar belakang atau *video streaming* resolusi tinggi melalui VPN, statistik volumetrik dan kepadatan paketnya terbaca oleh model memiliki kemiripan matematis dengan aktivitas interaktif pada perjudian online di ruang laten. Keterbatasan visibilitas akibat enkripsi *tunneling* memaksa model untuk menebak hanya berdasarkan bentuk aliran (IAT dan *bytes*), sehingga memicu penurunan spesifisitas pada trafik normal bervolume tinggi. Ikhtiasr akurasi per skenario dapat dilihat pada Tabel 4.

Tabel 4 Ikhtisar Akurasi Pendeteksian Per Skenario

Skenario	**Label**	**Total Data**	**Prediksi Benar**	**Akurasi (%)**
VPN	Judol	2.494	2.378	95,35%
DoH	Judol	2.597	2.420	93,18%
DoT	Judol	2.780	2.602	93,06%
Phone	Judol	1.825	1.806	98,96%
VPN	Normal	1.811	1.474	81,39%
None	Normal	3.879	3.646	93,99%

3.4. Hasil Pengembangan Sistem dan Pengujian Fungsionalitas

Implementasi agen IPS (*Intrusion Prevention System*) berbasis antarmuka web Svelte sukses menyajikan pemantauan *real-time*. Tampilan *dashboard* utama pada Gambar 9 merender baris-baris log tabel yang berisi alamat sumber, status probabilitas, dan keputusan pemblokiran seketika melalui komunikasi *WebSocket*.



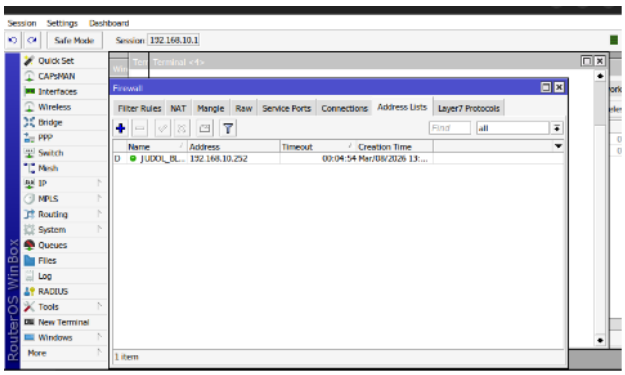
Gambar 9 Dashboard Svelte dengan Log Sistem

Evaluasi fungsionalitas sistem pada kondisi lapangan memvalidasi bahwa agen IPS mampu melakukan klasifikasi secara berkesinambungan (*continuous monitoring*). Pengujian menunjukkan bahwa waktu akumulasi (*detection window*) yang dibutuhkan sistem untuk mengumpulkan profil statistik yang memadai guna menyeberangi ambang batas penalti berada di kisaran 20 hingga 30 menit. Rentang waktu ini diterapkan secara sengaja untuk memastikan sistem tidak salah memblokir pengguna normal akibat *burst* trafik sesaat. Meskipun demikian, ketika batas skor penalti tercapai, *latency* pengiriman instruksi via API menuju *router* MikroTik tereksekusi instan secara *near real-time* (kurang dari 1 detik). Berdasarkan pengujian lapangan dengan 10 kali percobaan pada masing-masing kategori, tingkat keberhasilan deteksi (*True Positive*) untuk aktivitas perjudian online menggunakan teknik penyamaran (VPN, DoH, DoT) mencapai rasio 8/10 percobaan.

Pada simulasi observasi lapangan di Tabel 5kaantitatif, ketika probabilitas aktivitas terlarang melampaui skor batas penalti, *backend* langsung mengirim instruksi penjatuhan koneksi ke MikroTik. Tangkapan layar antarmuka Winbox pada Gambar 10 membuktikan keberhasilan instruksi API tersebut, di mana alamat *IP* target terekam otomatis ke dalam *Address-List* bernama `JUDOL_BLOCKED` untuk dieksekusi pengalihan aksesnya (*redirect*).

Tabel 5 Ringkasan Hasil Observasi Lapangan

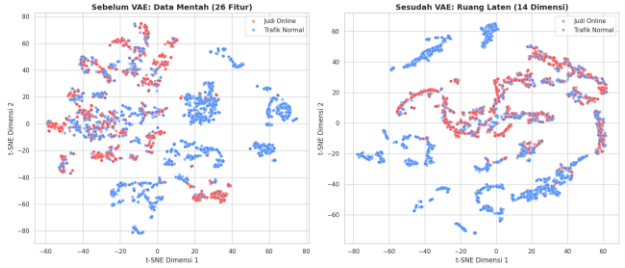
Kategori	**Skenario**	**Rasio percobaan berlabel judi *online***	**Karakteristik Data**
Normal (*Browsing/App*)	None, VPN, DoH, DoT	1/10	Tinggi & Fluktiatif
Perjudian *Online* (*Browser/App)*	VPN, DoH, DoT	8/10	Rendah & Konsisten
Game *Mobile*/PC	None (*Direct*)	4/10	Rendah & Konsisten
Idling (Diam)	None	0/10	Sangat Rendah



Gambar 10 Address-List yang terdaftar pada Winbox

3.5. Pembahasan Temuan Eksperimen

Penelitian ini secara nyata membuktikan keandalan analisis anomali statistik berbasis VAE-DNN sebagai solusi atas kelemahan DPI (*Deep Packet Inspection*) dalam membaca muatan trafik tersandi. Analisis proyeksi t-SNE (*t-Distributed Stochastic Neighbor Embedding*) pada Gambar 11 secara jelas mengonfirmasi bahwa arsitektur ekstraktor VAE memiliki kemampuan luar biasa untuk mengklasterisasi aliran anomali judi *online* dari lalu lintas aktivitas web normal di dalam dimensi ruang laten, tanpa perlu membuka enkripsi paket.



Gambar 11 Visualisasi t-SNE

Secara karakteristik, analisis profil transmisi menunjukkan adanya perbedaan pola fundamental antara lalu lintas judi *online* dan game *online* biasa. Aktivitas judi *online* terbukti menghasilkan muatan paket yang lebih seragam akibat dominasi elemen visual yang statis, berbeda dengan game online yang distribusi ukuran paketnya jauh lebih tersebar akibat variasi instruksi kontrol dan pembaruan lingkungan permainan. Perbedaan krusial lainnya terletak pada penggunaan protokol; game online memiliki kepadatan tinggi pada protokol UDP demi sinkronisasi status permainan *real-time* berlatensi rendah,

sedangkan judi online sangat mendominasi protokol TCP. Hal ini mengonfirmasi bahwa platform perjudian mutlak memprioritaskan keandalan pengiriman data (*data reliability*) guna memastikan transaksi taruhan dan pembaruan saldo terekam sempurna tanpa kehilangan paket.

Tabel 6 Perbandingan Karakteristik Trafik Judi *Online* dan *Game Online*

Karakteristik Parameter	**Judi *Online***	**Game *Online***
Parameter Statistik Trafik	Perjudian Online (Web/App)	Gim Daring (Mobile/PC)
Rata-rata Durasi Flow	± 120.000 – 350.000 ms *(Sesi interaksi per putaran/halaman)*	± 600.000+ ms *(Sesi permainan berkelanjutan)*
Jumlah Paket (*Bidirectional Packets*)	45 – 120 paket / *flow (Moderat dan stabil)*	350 – 1.200+ paket / *flow (Lonjakan tinggi)*
Ukuran Paket Rata-rata (*Mean Packet Size*)	550 – 900 bytes *(Didominasi HTTPS/TCP)*	80 – 250 bytes *(Didominasi datagram kecil)*
Rasio Protokol (TCP vs UDP)	98% TCP / 2% UDP	15% TCP / 85% UDP
Jeda Antar Paket (*IAT / Inter-Arrival Time*)	± 250 – 600 ms *(Jeda konsisten siklus taruhan)*	± 20 – 80 ms *(Sangat rapat dan fluktuatif)*

Pada Tabel 6, Game *online* mayoritas menggunakan UDP untuk memprioritaskan kecepatan transmisi interaksi *real-time* tanpa memedulikan paket yang hilang (*packet loss*). Sebaliknya, aplikasi perjudian online mutlak membutuhkan protokol TCP (HTTPS atau *WebSockets*) untuk memastikan integritas data transaksi dan sinkronisasi saldo yang tidak boleh terputus.

Analisis mendalam pada skenario VPN mengungkap adanya kelemahan sistem akibat fenomena tumpang tindih fitur (*feature overlapping*) yang sangat signifikan. Enkripsi proksi VPN secara kuat mengubah dan menyamarkan pola distribusi paket aslinya, sehingga karakteristik aliran data dari aktivitas perjudian tersamarkan dan menyerupai lalu lintas wajar. Akibat dari tumpang tindih ini, saat dilakukan uji coba sistem secara *real-time*, model terbukti mengalami kendala dan tidak dapat mendeteksi sebagian aktivitas perjudian online secara konsisten. Kondisi ini tercermin dari nilai akumulasi penalti klien yang stabil tanpa fluktuasi berarti, sehingga sistem gagal mencapai ambang batas (*threshold*) yang diperlukan untuk memicu eksekusi pemblokiran otomatis.

3.6. Keterbatasan Penelitian

Secara konseptual, penelitian ini memperbarui ruang lingkup teori operasional IPS dari sekadar penahan serangan siber eksternal menjadi filter penegakan kebijakan internal jaringan. Integrasi otomatis via API membuktikan mitigasi dapat dieksekusi instan tanpa menguras sumber daya *router* MikroTik. Namun demikian, uji coba sistem secara *real-time* mengungkap dua tantangan utama terkait generalisasi model.

Pertama, model menunjukkan indikasi *device overfitting*. Ketika diuji menggunakan perangkat keras asing yang tidak dilibatkan saat pengumpulan *dataset*, sistem gagal mendeteksi aktivitas judi online jika perangkat tersebut beroperasi secara independen. Fenomena ini diindikasikan berasal dari model VAE-DNN yang secara tidak sengaja mempelajari pola *noise* latar belakang dari perangkat keras asli, serta adanya peleburan probabilitas trafik antar-klien yang diproses dalam satu jendela waktu yang sama di *buffer backend*.

Kedua, sistem memiliki keterbatasan generalisasi lintas platform (*cross-platform generalization limit*). Ketika diuji pada platform penyedia permainan (*provider*) yang berbeda dari data pelatihan, fluktuasi skor penalti tertahan dan gagal menyentuh ambang batas pemblokiran. Hal ini membuktikan bahwa setiap platform perjudian menggunakan arsitektur *backend* dan protokol sinkronisasi yang berbeda,

yang terbaca oleh model sebagai distribusi data asing. Meskipun demikian, observasi lapangan menunjukkan bahwa model tetap konsisten mengenali arsitektur jaringan inti (*core engine*) selama masih berada dalam platform penyedia yang sama, sehingga administrator tidak perlu memperbarui *dataset* secara berkala untuk judul permainan baru. Lebih lanjut, rentang waktu deteksi antara 10 hingga 30 menit merupakan indikator positif bahwa agen IPS berbasis AI bekerja secara hati-hati dalam mengakumulasi bukti statistik profil paket guna memastikan tingkat presisi yang tinggi dan mencegah terjadinya *false positive*.

4. PENUTUP

4.1. Kesimpulan

Penelitian ini berhasil merancang dan mengimplementasikan IPS (*Intrusion Prevention System*) cerdas berbasis kecerdasan buatan untuk mengidentifikasi dan mencegah lalu lintas judi online di jaringan komunitas. Arsitektur hibrida VAE (*Variational Autoencoder*) dan DNN (*Deep Neural Network*) terbukti kapabel mengekstraksi anomali fitur statistik temporal dan volumetrik tanpa perlu mendekripsi muatan paket. Pada hasil evaluasi klasifikasi keseluruhan, model ini mencetak tingkat akurasi sebesar 80,80%, dengan nilai spesifik presisi 0,69, recall 0,91, dan nilai F1-Score 0,78 untuk pendeteksian label judi online. Secara implementasi, sistem ini responsif mengeksekusi mitigasi secara proaktif (*near real-time*) via API ke router MikroTik. Eksekusi beroperasi optimal dengan mendaftarkan IP target ke Address-List dan menerapkan aturan NAT untuk pengalihan (*redirect*) koneksi pada antarmuka bridge utama, di mana pengalihan ini berfokus pada lalu lintas HTTP. Esensi dari temuan ini menegaskan bahwa analisis anomali statistik mampu memodifikasi fungsi IPS tradisional menjadi penegak kebijakan jaringan internal yang tangguh terhadap proksi. Walaupun memiliki tantangan generalisasi lintas platform penyedia, model ini terbukti memiliki keandalan jangka panjang yang konsisten dalam mendeteksi berbagai variasi permainan dari arsitektur platform yang telah dikenalnya.

4.2. Saran

Untuk pengembangan di masa mendatang, disarankan agar metodologi evaluasi menerapkan pendekatan pengujian *leave-one-device-out* atau *leave-one-provider-out* secara ketat. Pendekatan ini diperlukan untuk menguji ketangguhan dan objektivitas model ketika dihadapkan pada infrastruktur perjudian online baru yang sama sekali belum pernah dilihat, guna memastikan bahwa IPS tidak mengalami *overfitting* terhadap profil perangkat keras atau infrastruktur *hosting* tertentu.

5. DAFTAR PUSTAKA

Mayradevi, I.A.P. and Tobing, D.H. 2024. Faktor-faktor yang Memengaruhi Perilaku Judi Online pada Remaja: Narrative Literature Review. *Jurnal Psikologi Perseptual* 9(1), pp. 4–26. doi: 10.24176/perseptual.v9i1.11940.

Gu, Z., Gou, G., Liu, C., Yang, C., Zhang, X., Li, Z. and Xiong, G. 2024. Let gambling hide nowhere: Detecting illegal mobile gambling apps via heterogeneous graph-based encrypted traffic analysis. *Computer Networks* 243, p. 110278. doi: 10.1016/j.comnet.2024.110278.

Antonio, J.C., Ong, A.K.S., Diaz, J.F.T., Cahigas, M.M.L. and Gumasing, Ma.J.J. 2025. The perceived risk and return, curiosity, and control analysis of online gambling intention among Gen Z and Millennials using extended UTAUT3. *Entertainment Computing* 52(1), p. 100918. doi: 10.1016/j.entcom.2024.100918

Monroy, S.S., Gupta, A.K. and Wahlstedt, G. 2023. Detection of Malicious DNS-over-HTTPS Traffic: An Anomaly Detection Approach using Autoencoders. doi: 10.48550/arXiv.2310.11325.

Alkasassbeh Mouhammd and Almseidin, M. 2023. Machine Learning Techniques for Accurately Detecting the DNS Tunneling. In: Arai, K. ed. *Intelligent Computing*. Cham: Springer Nature Switzerland 711(1), pp. 352–364. doi: 10.1007/978-3-031-37717-4_24.

Alzighaibi, A.R. 2023. Detection of DoH Traffic Tunnels Using Deep Learning for Encrypted Traffic Classification. *Computers* 12(3), pp. 47–57. doi: 10.3390/computers12030047.

Guerra-Manzanares, A., Caprolu, M. and Di Pietro, R. 2025. A comprehensive review on machine learning-based VPN detection: Scenarios, methods, and open challenges. *Computer Science Review* 58, p. 100781. doi: 10.1016/j.cosrev.2025.100781.

Azam, Z., Islam, Md.M. and Huda, M.N. 2023. Comparative Analysis of Intrusion Detection Systems and Machine Learning-Based Model Analysis Through Decision Tree. *IEEE Access* 11(10185955), pp. 80348–80391. doi: 10.1109/ACCESS.2023.3296444.

Abuajwa, O., Hassan, S.M.B.M., Mahmud, A. Bin and Aziz, A.B.A. 2025. Deep Packet Inspection (DPI) Technologies and Their Role in Cyber Threat Detection. In: *Multimedia University Engineering Conference (MECON)*. pp. 1–7. doi: 10.1109/MECON67253.2025.11276900.

Syafi'i Bachtiar, M., Rahaningsih, N. and Dana, R.D. 2024. FIREWALL FILTERING BERBASIS DEEP PACKET INSPECTION DALAM MENDETEKSI DAN MENCEGAH ANCAMAN MALWARE. *Jurnal Mahasiswa Teknik Informatika* 8(1), pp. 399–405. doi: 10.36040/jati.v8i1.8387.

Sari, D.P., Halim, Z., Irlon, I., Waseso, B. and Saromah, S. 2024. Implementasi Machine Learning untuk Deteksi Intrusi pada Jaringan Komputer. *Jurnal Minfo Polgan* 13(2), pp. 1389–1394. doi: 10.33395/jmp.v13i2.14074.

Laghrissi, F., Douzi, S., Douzi, K. and Hssina, B. 2021. Intrusion detection systems using long short-term memory (LSTM). *Journal of Big Data* 8(1), p. 65. doi: 10.1186/s40537-021-00448-4.

Alwhbi, I.A., Zou, C.C. and Alharbi, R.N. 2024. Encrypted Network Traffic Analysis and Classification Utilizing Machine Learning. *Sensors* 24(11), pp. 1–17. doi: 10.3390/s24113509.

Rahayu Prasiska. 2025. *Klasifikasi Traffic Jaringan Online Gambling Berbasis Deep Learning*. Skripsi. Sistem Komputer. Universitas Sriwijaya.

Yang, G., Wu, B., He, J., Ni, L. and Xia, T. 2025. Towards Reliable Detection of Malicious DNS-over-HTTPS (DoH) Tunneling Traffic Under Low-Quality Training Data. pp. 423–434. doi: 10.1007/978-981-96-9872-1_35.

Hasin, M., Havrilla, M. and Chovancová, E. 2023. Detection of HTTP DDoS Attacks Using NFStream and TensorFlow. *Applied Sciences* 13(11), pp. 6665–6671. doi: 10.3390/app13116671.

Correia, L., Goos, J.-C., Klein, P., Bäck, T. and Kononova, A. V. 2025. TeVAE: A Variational Autoencoder Approach for Discrete Online Anomaly Detection in Variable-State Multivariate Time-Series Data. In: *Computational Intelligence*. Springer Nature Switzerland 1196, pp. 106–132. doi: 10.1007/978-3-031-85252-7_7.

Vasudev Karthik Ravindran, Sharad Shyam Ojha and Arvind Kamboj. 2025. A Comparative Analysis of Signature-Based and Anomaly-Based Intrusion Detection Systems. *International Journal of Latest Technology in Engineering Management & Applied Science* 14(5), pp. 209–214. doi: 10.51583/IJLTEMAS.2025.140500026.

Karuna Jyothi, K. and Reddy, B.I. 2023. CSEIT1835225 | Study on Virtual Private Network (VPN), VPN's Protocols And Security Study on Virtual Private Network (VPN), VPN's Protocols And Security. *International Journal of Scientific Research in Computer Science, Engineering and Information Technology* 3(5). pp. 919-932 Available at: https://www.researchgate.net/publication/368831275.

Scourfield, M., Saintonge, A., de Mijolla, D. and Viti, S. 2023. De-noising of galaxy optical spectra with autoencoders. *Monthly Notices of the Royal Astronomical Society* 526(2), pp. 3037–3050. doi: 10.1093/mnras/stad2709.

Domínguez-Morales, M., Civit-Masot, J., Muñoz-Saavedra, L. and Damaševičius, R. 2024. *Deep Learning*. London: IntechOpen. doi: 10.5772/intechopen.107725.

Eman Jawad. 2023. THE DEEP NEURAL NETWORK-A REVIEW. *JOURNAL OF MATHEMATICS* 9(9), pp. 1–5. doi: 10.53555/m.v9i9.5842.

Vujovic, Ž.Đ. 2021. Classification Model Evaluation Metrics. *International Journal of Advanced Computer Science and*

Applications 12(6). pp. 599-606. doi: https://dx.doi.org/10.14569/IJACSA.2021.0120670.