JURIKOM (Jurnal Riset Komputer), Vol. 13 No. 2, April 2026
e-ISSN 2715-7393 (Media Online), p-ISSN 2407-389X (Media Cetak)
DOI 10.30865/jurikom.v13i2.9662
Hal 513-525
https://ejurnal.stmik-budidarma.ac.id/index.php/jurikom

Pemodelan Intrusion Detection System Menggunakan CNN-LSTM dengan Selective SMOTE Untuk Deteksi Serangan Pada Data Tidak Seimbang

Arya Satrya Wicaksana*, Robert Marco

Fakultas Ilmu Komputer, PJJ Informatika, Universitas Amikom Yogyakarta, Yogyakarta, Indonesia
Email: [1,*]aryasatrya@students.amikom.ac.id, [2]robertmarco@amikom.ac.id
Email Penulis Korespondensi: aryasatrya@students.amikom.ac.id
Submitted **20-03-2025;** Accepted **06-04-2026;** Published **30-04-2026**

Abstrak

Intrusion Detection System (IDS) merupakan komponen penting dalam menjaga keamanan jaringan dari berbagai serangan siber yang semakin kompleks. Salah satu tantangan utama dalam pengembangan IDS berbasis machine learning adalah ketidakseimbangan data (imbalanced data) yang menyebabkan penurunan kemampuan model dalam mendeteksi serangan, khususnya pada kelas minoritas. Penelitian ini mengusulkan peningkatan performa IDS berbasis deep learning menggunakan arsitektur hybrid CNN-LSTM yang dipadukan dengan metode Selective SMOTE berbasis prevalence ratio, yaitu pendekatan oversampling yang dilakukan secara selektif berdasarkan tingkat ketimpangan masing-masing kelas. Dataset yang digunakan adalah NSL-KDD dengan tahapan preprocessing meliputi encoding fitur kategorikal dan normalisasi fitur numerik. Evaluasi dilakukan dengan membandingkan model CNN–LSTM baseline dan CNN-LSTM dengan Selective SMOTE menggunakan metrik accuracy, precision, recall, specificity, dan F1-score. Hasil eksperimen menunjukkan bahwa model baseline menghasilkan accuracy sebesar 0.9947 dengan macro recall 0.8080, sedangkan penerapan Selective SMOTE meningkatkan macro recall menjadi 0.8929 dan F1-score menjadi 0.8515, terutama pada kelas minoritas seperti U2R dan R2L. Meskipun accuracy sedikit menurun menjadi 0.9946, nilai specificity tetap tinggi sebesar 0.9981 dengan false positive rate yang rendah. Hasil ini menunjukkan bahwa metode Selective SMOTE efektif dalam meningkatkan sensitivitas deteksi serangan tanpa menurunkan performa keseluruhan sistem IDS secara signifikan.

Kata Kunci: Intrusion Detection System; CNN-LSTM; Selective SMOTE; Imbalanced Data; Deep Learning; NSL-KDD

Abstract

An Intrusion Detection System (IDS) is a critical component in safeguarding network security against increasingly complex cyberattacks. One of the main challenges in developing machine learning-based IDS is data imbalance, which reduces the model's ability to detect attacks, particularly in the minority class. This study proposes improving the performance of deep learning-based IDS using a hybrid CNN-LSTM architecture combined with the prevalence ratio-based Selective SMOTE method, which is an oversampling approach performed selectively based on the imbalance level of each class. The dataset used is NSL-KDD, with preprocessing steps including categorical feature encoding and numerical feature normalization. Evaluation was conducted by comparing the baseline CNN–LSTM model and the CNN-LSTM with Selective SMOTE using the metrics accuracy, precision, recall, specificity, and F1-score. Experimental results show that the baseline model achieved an accuracy of 0.9947 with a macro recall of 0.8080, while the application of Selective SMOTE improved the macro recall to 0.8929 and the F1-score to 0.8515, particularly for minority classes such as U2R and R2L. Although accuracy decreased slightly to 0.9946, the specificity remained high at 0.9981 with a low false positive rate. These results indicate that the Selective SMOTE method is effective in improving attack detection sensitivity without significantly degrading the overall performance of the IDS system.

Keywords: Intrusion Detection System; CNN-LSTM; Selective SMOTE; Imbalanced Data; Deep Learning; NSL-KDD

1. PENDAHULUAN

Perkembangan teknologi jaringan dan meningkatnya kompleksitas infrastruktur digital telah menyebabkan lanskap ancaman siber menjadi semakin beragam dan dinamis. Serangan modern tidak hanya meningkat dari sisi volume, tetapi juga dari variasi teknik dan tingkat kecanggihannya, terutama dalam konteks sistem yang semakin terhubung seperti IoT, cloud, dan cyber-physical systems, sehingga kebutuhan IDS yang akurat sekaligus dapat dipercaya menjadi semakin penting [1]. Kondisi ini menjadikan mekanisme pengamanan jaringan konvensional berbasis signature semakin tidak memadai, khususnya untuk mendeteksi serangan baru (unknown/zero-day) maupun anomali kompleks yang belum terdokumentasi, sehingga pendekatan IDS berbasis pembelajaran mesin dan deep learning menjadi fokus penelitian untuk mempelajari pola serangan secara otomatis dari data jaringan [2].

Ketertarikan terhadap tema ini didorong oleh fakta bahwa meskipun berbagai model deep learning menunjukkan performa yang tinggi pada eksperimen, penerapan IDS di lingkungan nyata masih menghadapi tantangan serius, terutama terkait ketidakseimbangan data (imbalanced data) dan keberadaan noise pada lalu lintas jaringan. Distribusi data IDS yang umumnya didominasi trafik normal membuat model cenderung bias terhadap kelas mayoritas dan kurang sensitif dalam mengenali serangan minoritas yang bersifat kritis, sehingga meningkatkan risiko false negative [2].

Tantangan ini dapat semakin berat ketika serangan bersifat tersembunyi atau tidak memiliki pola yang jelas pada sistem konvensional, sehingga menuntut strategi pemodelan yang mampu menangani kompleksitas data dan dinamika ancaman secara lebih efektif [3]. Sejalan dengan perkembangan riset, studi-studi yang dikaji menunjukkan bahwa pendekatan deep learning berbasis arsitektur hibrida, khususnya kombinasi Convolutional Neural Network (CNN) dan Long Short-Term Memory (LSTM), efektif untuk meningkatkan kinerja deteksi intrusi karena mampu mengekstraksi fitur spasial dan temporal secara simultan. Kombinasi CNN-LSTM dilaporkan unggul pada berbagai dataset IDS standar melalui integrasi teknik seperti standardization, batch normalization, dan dropout, yang membantu pembelajaran fitur dan stabilitas pelatihan [4]. Secara lebih umum, teknik deep learning seperti CNN, LSTM, dan autoencoder juga dilaporkan

JURIKOM (Jurnal Riset Komputer), Vol. 13 No. 2, April 2026
e-ISSN 2715-7393 (Media Online), p-ISSN 2407-389X (Media Cetak)
DOI 10.30865/jurikom.v13i2.9662
Hal 513-525
https://ejurnal.stmik-budidarma.ac.id/index.php/jurikom

konsisten melampaui metode machine learning tradisional karena kemampuan mempelajari fitur secara otomatis dan adaptif terhadap variasi ancaman [5].

Namun demikian, kajian literatur juga menegaskan bahwa sebagian penelitian masih memiliki keterbatasan pada aspek robustness. Pada praktiknya, strategi peningkatan performa awal seperti penerapan SMOTE dan dropout dapat membantu, tetapi belum selalu cukup untuk menghadapi perubahan pola data dunia nyata secara berkelanjutan, khususnya ketika data mengandung noise dan distribusinya tidak stabil [6]. Selain itu, permasalahan imbalanced data yang melekat pada IDS juga menuntut evaluasi yang lebih komprehensif agar kinerja model tidak hanya "baik" pada akurasi global, tetapi juga benar-benar sensitif dalam mendeteksi serangan minoritas dan tidak menghasilkan false alarm berlebihan pada trafik normal [2].

Selain ketidakseimbangan dan noise, sistem IDS juga menghadapi tantangan tingginya dimensi fitur serta redundansi atribut yang dapat meningkatkan kompleksitas model, memperpanjang waktu pelatihan, dan menurunkan akurasi bila fitur tidak relevan ikut dipelajari. Kondisi ini telah dilaporkan dapat menurunkan kinerja model pada skenario IDS tertentu karena overhead komputasi meningkat dan proses pembelajaran terganggu oleh fitur yang tidak informatif [7]. Oleh karena itu, diperlukan perancangan model IDS yang tidak hanya akurat, tetapi juga efisien dan robust melalui integrasi teknik pemodelan yang mampu menangani kompleksitas data secara optimal [8][4].

Meskipun berbagai penelitian telah menunjukkan bahwa model deep learning, khususnya arsitektur hibrida CNN-LSTM, mampu mencapai tingkat akurasi yang sangat tinggi dalam deteksi intrusi, sebagian besar studi masih berfokus pada metrik akurasi sebagai indikator utama performa tanpa mengevaluasi secara komprehensif metrik lain seperti sensitivity (recall) dan specificity yang krusial dalam konteks IDS, terutama untuk mendeteksi serangan pada kelas minoritas [4][5]. Selain itu, banyak penelitian terkini lebih menitikberatkan evaluasi pada dataset IDS modern seperti CIC-IDS2017 dan UNSW-NB15, sementara validasi terhadap dataset benchmark klasik seperti NSL-KDD yang memiliki karakteristik distribusi data berbeda masih relatif terbatas, sehingga generalisasi model terhadap berbagai jenis dataset belum sepenuhnya teruji [9]. Di sisi lain, pendekatan penanganan imbalanced data umumnya masih menggunakan teknik oversampling konvensional seperti SMOTE secara global tanpa mempertimbangkan tingkat ketimpangan antar kelas secara spesifik, yang berpotensi menghasilkan distribusi sintetis yang kurang representatif dan dapat mempengaruhi stabilitas model [6][10].

Oleh karena itu, penelitian ini mengusulkan pengembangan model Intrusion Detection System berbasis deep learning menggunakan arsitektur CNN-LSTM dengan penerapan teknik SMOTE untuk mengatasi permasalahan ketidakseimbangan data. Berbeda dengan pendekatan sebelumnya, penelitian ini menitikberatkan pada evaluasi kinerja model secara komprehensif dengan mempertimbangkan keseimbangan antara sensitivity dan specificity. Penggunaan dataset NSL-KDD sebagai benchmark klasik juga bertujuan untuk menguji kemampuan generalisasi model pada karakteristik data yang tidak seimbang, sehingga diharapkan menghasilkan sistem IDS yang lebih adaptif dan andal dalam mendeteksi berbagai jenis serangan jaringan.

2. METODOLOGI PENELITIAN

2.1 Pendekatan Penelitian

Penelitian ini bersifat kuantitatif-eksperimental dengan pendekatan pemodelan dan evaluasi komparatif. Kajian berfokus pada pengembangan Intrusion Detection System (IDS) berbasis deep learning menggunakan arsitektur CNN-LSTM untuk mendeteksi intrusi pada data lalu lintas jaringan yang memiliki karakteristik utama yaitu ketidakseimbangan kelas (imbalanced). Pendekatan deep learning dipilih karena kemampuannya dalam mengekstraksi fitur kompleks serta menangkap pola spasial dan temporal secara simultan [11]. Untuk memastikan hasil yang dapat dibandingkan dan bersifat benchmark, eksperimen dilakukan menggunakan dataset IDS yang banyak digunakan dalam penelitian yaitu NSL-KDD, yang telah menjadi standar evaluasi dalam berbagai studi IDS berbasis machine learning dan deep learning[12], sehingga performa model dapat dianalisis secara lebih komprehensif dan representatif terhadap berbagai jenis serangan jaringan.

2.2 Skema Penelitian

Penelitian ini dirancang secara sistematis untuk mengembangkan dan mengevaluasi model Intrusion Detection System (IDS) berbasis deep learning menggunakan arsitektur CNN-LSTM dengan penerapan teknik Synthetic Minority Oversampling Technique (SMOTE). Tujuan utama dari tahapan penelitian ini adalah untuk menghasilkan model deteksi intrusi yang mampu meningkatkan kemampuan deteksi serangan jaringan, khususnya pada kondisi data yang tidak seimbang (imbalanced data), yang merupakan salah satu tantangan utama dalam pengembangan IDS modern [11][13].

Secara umum, tahapan penelitian dimulai dari proses pengumpulan dataset, dilanjutkan dengan pemrosesan data, penyeimbangan data menggunakan SMOTE, pembangunan model CNN-LSTM, pelatihan model, serta evaluasi performa model menggunakan metrik evaluasi yang telah ditentukan. Pendekatan berbasis deep learning dipilih karena kemampuannya dalam mengekstraksi fitur kompleks serta menangkap pola non-linear pada data jaringan secara lebih efektif dibandingkan metode konvensional [12].

Pada tahap awal, penelitian menggunakan dataset NSL-KDD yang merupakan dataset benchmark yang banyak digunakan dalam penelitian Intrusion Detection System. Dataset ini dipilih karena memiliki distribusi data yang lebih representatif dibandingkan dataset pendahulunya serta telah digunakan secara luas dalam berbagai penelitian IDS berbasis

JURIKOM (Jurnal Riset Komputer), Vol. 13 No. 2, April 2026
e-ISSN 2715-7393 (Media Online), p-ISSN 2407-389X (Media Cetak)
DOI 10.30865/jurikom.v13i2.9662
Hal 513-525
https://ejurnal.stmik-budidarma.ac.id/index.php/jurikom

machine learning dan deep learning [9]. Dataset NSL-KDD terdiri dari berbagai fitur yang merepresentasikan karakteristik lalu lintas jaringan, baik yang bersifat numerik maupun kategorikal.

Tahap berikutnya adalah pemrosesan data (data preprocessing) yang bertujuan untuk mempersiapkan dataset sebelum digunakan dalam proses pelatihan model. Proses ini meliputi pembersihan data, transformasi fitur kategorikal menggunakan teknik One-Hot Encoding, serta normalisasi fitur numerik menggunakan teknik standardization [4]. Tahap preprocessing ini sangat penting untuk memastikan bahwa data yang digunakan dalam proses pelatihan model berada dalam format yang sesuai dan tidak mengandung nilai yang dapat mengganggu proses pembelajaran.

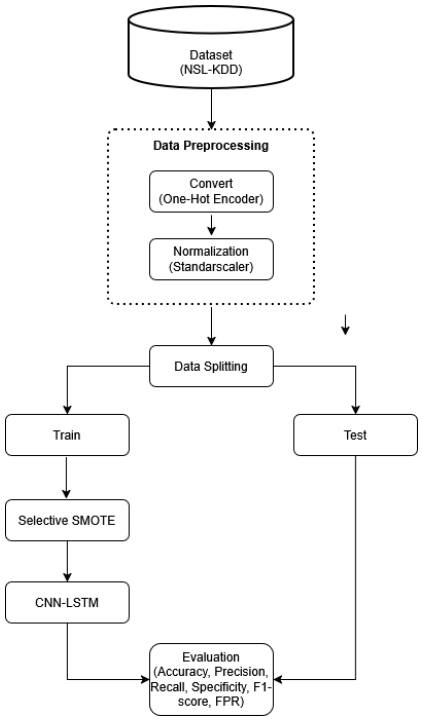
Setelah tahap preprocessing selesai dilakukan, langkah selanjutnya adalah menerapkan teknik SMOTE untuk mengatasi permasalahan ketidakseimbangan data pada dataset IDS. Teknik SMOTE bekerja dengan menghasilkan sampel sintetis pada kelas minoritas sehingga distribusi dataset menjadi lebih seimbang. Dengan distribusi data yang lebih seimbang, model pembelajaran diharapkan dapat mempelajari karakteristik serangan secara lebih efektif dan tidak bias terhadap kelas mayoritas[6].

Tahap berikutnya adalah pembangunan model deep learning menggunakan arsitektur CNN-LSTM. Pada tahap ini, CNN digunakan untuk mengekstraksi fitur penting dari data input melalui operasi konvolusi, sedangkan LSTM digunakan untuk mempelajari hubungan temporal dalam data lalu lintas jaringan. Kombinasi kedua arsitektur ini memungkinkan model untuk menangkap pola kompleks pada data jaringan sehingga dapat meningkatkan kemampuan deteksi intrusi[10].

Setelah model dibangun, dilakukan proses pelatihan (training) menggunakan data pelatihan yang telah diproses sebelumnya. Proses pelatihan ini bertujuan untuk menyesuaikan parameter model sehingga mampu mempelajari pola yang terdapat pada data jaringan. Selanjutnya, model yang telah dilatih akan diuji menggunakan data pengujian (testing data) untuk mengevaluasi kemampuan generalisasi model terhadap data yang tidak digunakan dalam proses pelatihan.

Tahap terakhir adalah evaluasi performa model menggunakan beberapa metrik evaluasi yang umum digunakan dalam penelitian IDS, seperti accuracy, precision, recall (sensitivity), specificity, F1-score, dan false positive rate (FPR). Evaluasi ini bertujuan untuk mengukur kemampuan model dalam mendeteksi serangan jaringan serta kemampuannya dalam membedakan trafik normal secara akurat.

Untuk memberikan gambaran yang lebih sistematis mengenai alur penelitian yang dilakukan, tahapan penelitian ini divisualisasikan dalam bentuk diagram alir seperti ditunjukkan pada Gambar 1. Diagram tersebut menggambarkan keseluruhan proses mulai dari pengolahan data hingga evaluasi model yang diusulkan.



Gambar 1. Diagram Alir Penelitian

2.3 Dataset

Dataset yang digunakan dalam penelitian ini adalah NSL-KDD, yang merupakan pengembangan dan penyempurnaan dari dataset KDD Cup 1999 (KDD'99) yang sebelumnya banyak digunakan dalam penelitian Intrusion Detection System (IDS). Dataset NSL-KDD dikembangkan untuk mengatasi beberapa kelemahan yang terdapat pada dataset KDD'99, khususnya terkait dengan masalah redundansi data dan distribusi sampel yang tidak seimbang. Pada dataset KDD'99, terdapat banyak data duplikat yang dapat menyebabkan model pembelajaran bias terhadap pola tertentu dan menghasilkan performa yang tidak representatif ketika diuji pada data baru. Oleh karena itu, NSL-KDD dirancang dengan

JURIKOM (Jurnal Riset Komputer), Vol. 13 No. 2, April 2026
e-ISSN 2715-7393 (Media Online), p-ISSN 2407-389X (Media Cetak)
DOI 10.30865/jurikom.v13i2.9662
Hal 513-525
https://ejurnal.stmik-budidarma.ac.id/index.php/jurikom

menghilangkan data duplikat serta menyusun ulang distribusi data sehingga evaluasi model dapat dilakukan secara lebih objektif dan adil[9].

Dataset NSL-KDD terdiri dari rekaman lalu lintas jaringan yang telah diklasifikasikan ke dalam dua kategori utama, yaitu trafik normal dan trafik serangan (attack). Setiap rekaman data dalam dataset ini direpresentasikan oleh 41 fitur input yang menggambarkan karakteristik koneksi jaringan, seperti durasi koneksi, jumlah paket yang dikirimkan, jenis protokol, serta berbagai indikator aktivitas jaringan lainnya. Fitur-fitur tersebut terdiri dari kombinasi fitur numerik dan fitur kategorikal yang merepresentasikan berbagai aspek perilaku lalu lintas jaringan[14]. Untuk memberikan gambaran yang lebih jelas mengenai struktur fitur yang digunakan dalam dataset NSL-KDD, pengelompokan fitur ditampilkan pada Tabel 1.

Tabel 1. Fitur Dataset NSL-KDD

Kelompok Fitur	Nama Fitur	Jumlah
Fitur Dasar (Basic Features)	duration, protocol_type, service, flag, src_bytes, dst_bytes, land, wrong_fragment, urgent	9
Fitur Konten (Content Features)	hot, num_failed_logins, logged_in, num_compromised, root_shell, su_attempted, num_root, num_file_creations, num_shells, num_access_files, num_outbound_cmds, is_host_login, is_guest_login	13
Fitur Waktu (Time Features)	count, srv_count, serror_rate, srv_serror_rate, rerror_rate, srv_rerror_rate, same_srv_rate, diff_srv_rate, srv_diff_host_rate	9
Fitur Trafik (Traffic Features)	dst_host_count, dst_host_srv_count, dst_host_same_srv_rate, dst_host_diff_srv_rate, dst_host_same_src_port_rate, dst_host_srv_diff_host_rate, dst_host_serror_rate, dst_host_srv_serror_rate, dst_host_rerror_rate, dst_host_srv_rerror_rate	10
Total Fitur		41

Berdasarkan Tabel 1, fitur dalam dataset NSL-KDD dikelompokkan ke dalam empat kategori utama, yaitu fitur dasar (basic features), fitur konten (content features), fitur waktu (time features), dan fitur trafik (traffic features), dengan total keseluruhan sebanyak 41 fitur. Pengelompokan ini memungkinkan model untuk mempelajari karakteristik lalu lintas jaringan dari berbagai aspek, baik dari sisi koneksi dasar hingga pola perilaku trafik yang lebih kompleks.

Dataset yang digunakan dalam penelitian ini total 125.973 data dengan klasifikasi serangan dalam empat kategori utama: Denial of Service (DoS), Probe, Remote to Local (R2L), dan User to Root (U2R). Kemudian dibagi menjadi tiga bagian utama, yaitu 80.622 data digunakan sebagai data latih (training data) untuk melatih model CNN-LSTM dalam mempelajari pola lalu lintas jaringan, 20.156 data digunakan sebagai data validasi (validation data) yang berfungsi untuk mengevaluasi performa model selama proses pelatihan serta membantu dalam proses penyesuaian parameter model dan 25.195 data digunakan sebagai data uji (testing data) yang bertujuan untuk mengukur kemampuan generalisasi model terhadap data yang tidak digunakan dalam proses pelatihan. Untuk memberikan gambaran distribusi data pada masing-masing kategori serangan, rincian jumlah data latih, validasi, dan uji ditampilkan pada Tabel 2.

Tabel 2. Kategori dan Nama Serangan pada Dataset NSL-KDD

Kategori Serangan	Nama Serangan	Data Latih	Data Validasi	Data Uji
Normal	normal	43099	10775	13469
DoS	back, land, neptune, pod, smurf, teardrop	29393	7348	9186
Probe	ipsweep, nmap, portsweep, satan	7460	1865	2331
R2L	ftp_write, guess_passwd, imap, multihop, phf, spy, warezclient, warezmaster	637	159	199
U2R	buffer_overflow, loadmodule, perl, rootkit	33	9	10
Total		80622	20156	25195

Berdasarkan Tabel 2, terlihat bahwa distribusi data antar kelas bersifat tidak seimbang (imbalanced), di mana kelas Normal dan DoS memiliki jumlah data yang jauh lebih besar dibandingkan kelas minoritas seperti R2L dan U2R. Ketimpangan distribusi ini berpotensi menyebabkan model cenderung bias terhadap kelas mayoritas dan kurang optimal dalam mendeteksi serangan pada kelas minoritas. Kondisi ini menjadi salah satu tantangan utama dalam pengembangan Intrusion Detection System (IDS) karena serangan dengan frekuensi rendah seperti U2R dan R2L justru memiliki tingkat risiko yang tinggi namun sulit dideteksi. Oleh karena itu, diperlukan pendekatan khusus seperti teknik resampling untuk meningkatkan representasi kelas minoritas sehingga model dapat mempelajari pola serangan secara lebih seimbang dan akurat.

2.4 Pemrosesan Data

JURIKOM (Jurnal Riset Komputer), Vol. 13 No. 2, April 2026
e-ISSN 2715-7393 (Media Online), p-ISSN 2407-389X (Media Cetak)
DOI 10.30865/jurikom.v13i2.9662
Hal 513-525
https://ejurnal.stmik-budidarma.ac.id/index.php/jurikom

Tahap pemrosesan data (data preprocessing) dilakukan untuk mempersiapkan dataset NSL-KDD agar dapat digunakan secara optimal dalam proses pelatihan model deep learning. Proses ini bertujuan untuk memastikan bahwa data berada dalam format yang sesuai, bebas dari nilai yang tidak valid, serta memiliki skala yang seragam sehingga dapat meningkatkan stabilitas dan kinerja model selama proses pembelajaran[14].

a. Labeling

Pada tahap ini dilakukan identifikasi terhadap kolom label yang berfungsi sebagai target klasifikasi dalam penelitian. Kolom label menunjukkan apakah suatu koneksi jaringan termasuk trafik normal atau jenis serangan tertentu. Label ini menjadi variabel target yang akan diprediksi oleh model CNN-LSTM selama proses pelatihan dan pengujian[15].

b. Mapping Attack Classes

Dataset NSL-KDD memiliki berbagai jenis serangan yang berbeda. Untuk menyederhanakan proses klasifikasi dan mempermudah analisis hasil, setiap jenis serangan dipetakan ke dalam lima kelas utama, yaitu Normal, Denial of Service (DoS), Probe, Remote to Local (R2L), dan User to Root (U2R). Proses mapping ini dilakukan dengan mengelompokkan setiap jenis serangan ke dalam kategori serangan yang sesuai sehingga model dapat mempelajari pola serangan pada tingkat kelas yang lebih umum[16].

c. Cleaning

Setelah proses mapping label dilakukan, tahap selanjutnya adalah menghapus data atau atribut yang tidak diperlukan dalam proses pelatihan model. Proses ini bertujuan untuk mengurangi kompleksitas dataset serta menghindari penggunaan fitur yang tidak memberikan kontribusi signifikan terhadap proses klasifikasi. Dengan menghilangkan atribut yang tidak relevan, proses pembelajaran model menjadi lebih efisien dan risiko overfitting dapat diminimalkan.

d. Encoding

Dataset NSL-KDD memiliki beberapa fitur kategorikal seperti protocol_type, service, dan flag. Fitur-fitur tersebut tidak dapat langsung diproses oleh model deep learning karena masih berupa nilai kategorikal. Oleh karena itu dilakukan transformasi menggunakan teknik One-Hot Encoding, yaitu mengubah setiap kategori menjadi representasi numerik dalam bentuk vektor biner. Proses ini memungkinkan model CNN-LSTM memproses data kategorikal tanpa mengasumsikan adanya hubungan ordinal antar kategori.

e. Normalization

Setelah proses encoding selesai dilakukan, tahap berikutnya adalah normalisasi fitur numerik. Normalisasi bertujuan untuk menyamakan skala nilai antar fitur sehingga tidak terjadi dominasi nilai pada fitur tertentu selama proses pelatihan model. Dalam penelitian ini menggunakan StandarScaler, yaitu mengubah distribusi nilai fitur sehingga memiliki rata-rata mendekati nol dan standar deviasi satu. Proses ini dilakukan dengan mengurangi nilai setiap fitur dengan nilai rata-ratanya dan kemudian membaginya dengan standar deviasi dari fitur tersebut.

f. Data Splitting

Dataset yang telah diproses kemudian dibagi menjadi tiga bagian utama yaitu data pelatihan, data validasi, dan data pengujian. Data pelatihan digunakan untuk melatih model CNN-LSTM dalam mempelajari pola lalu lintas jaringan, data validasi digunakan untuk memantau performa model selama proses pelatihan, sedangkan data pengujian digunakan untuk mengevaluasi kemampuan generalisasi model terhadap data yang belum pernah digunakan sebelumnya. Pada penelitian ini, dataset dibagi menggunakan rasio 80:20, di mana 80% data digunakan sebagai data pelatihan (training data) dan 20% sisanya digunakan sebagai data pengujian (testing data), kemudian sebagian dari data pelatihan dipisahkan kembali untuk digunakan sebagai data validasi (validation data)[4].

g. Resampling (SMOTE)

Tahap terakhir dalam preprocessing adalah penerapan teknik SMOTE pada data pelatihan. Dataset IDS umumnya memiliki distribusi kelas yang tidak seimbang, di mana jumlah data trafik normal jauh lebih banyak dibandingkan beberapa jenis serangan minoritas seperti R2L dan U2R. SMOTE bekerja dengan menghasilkan sampel sintetis pada kelas minoritas melalui proses interpolasi antar data yang ada sehingga distribusi dataset menjadi lebih seimbang. Dengan distribusi data yang lebih seimbang, model CNN-LSTM diharapkan dapat mempelajari karakteristik setiap kelas serangan secara lebih efektif dan meningkatkan kemampuan deteksi terhadap serangan minoritas. Proses penerapan SMOTE dalam penelitian ini menggunakan threshold sebesar 0,5% dari jumlah data pada kelas mayoritas. Kelas yang memiliki jumlah data di bawah threshold tersebut dianggap sebagai kelas minoritas yang perlu dilakukan proses oversampling. Selanjutnya, jumlah data pada kelas minoritas tersebut ditingkatkan dengan faktor pengali sebesar 10 kali lipat untuk memberikan variasi data pada kelas tersebut[10].

2.5 Resampling Menggunakan Synthetic Minority Oversampling Technique (SMOTE)

Ketidakseimbangan data merupakan permasalahan umum pada dataset Intrusion Detection System (IDS), termasuk pada dataset NSL-KDD, di mana jumlah data pada kelas mayoritas seperti Normal dan DoS jauh lebih besar dibandingkan kelas minoritas seperti R2L dan U2R. Kondisi ini dapat menyebabkan model pembelajaran menjadi bias terhadap kelas mayoritas sehingga kemampuan model dalam mendeteksi serangan minoritas menjadi rendah. Untuk mengatasi

JURIKOM (Jurnal Riset Komputer), Vol. 13 No. 2, April 2026
e-ISSN 2715-7393 (Media Online), p-ISSN 2407-389X (Media Cetak)
DOI 10.30865/jurikom.v13i2.9662
Hal 513-525
https://ejurnal.stmik-budidarma.ac.id/index.php/jurikom

permasalahan tersebut, penelitian ini menerapkan metode Synthetic Minority Oversampling Technique (SMOTE) yang diperkenalkan oleh [6][10].

SMOTE bekerja dengan menghasilkan sampel sintetis pada kelas minoritas melalui proses interpolasi antara data yang berdekatan dalam ruang fitur. Proses ini dimulai dengan memilih sebuah sampel dari kelas minoritas secara acak yang dinotasikan sebagai x_0, kemudian sistem menentukan K-nearest neighbors dari sampel tersebut. Salah satu tetangga terdekat kemudian dipilih secara acak dan dinotasikan sebagai x_κ. Sampel sintetis baru dibentuk melalui proses interpolasi linier menggunakan persamaan berikut:

$$z = x_0 + \omega(x_\kappa - x_0) \quad (1)$$

Dimana z merupakan sampel sintetis yang dihasilkan dan ω merupakan nilai acak pada rentang 0 hingga 1. Dengan cara ini, SMOTE menghasilkan data baru yang berada di antara dua sampel minoritas sehingga dapat meningkatkan jumlah dan variasi data tanpa hanya menduplikasi data yang sudah ada. Dalam penelitian ini, penerapan SMOTE dilakukan secara selektif berdasarkan nilai class prevalence ratio untuk menentukan kelas minoritas yang memerlukan proses oversampling. Nilai prevalence ratio dihitung menggunakan persamaan berikut:

$$Class\ Prevalence\ Ratio = 100 \times \frac{Jumlah\ data\ pelatihan\ pada\ kelas\ tertentu}{Total\ jumlah\ data\ pelatihan} \quad (2)$$

Nilai tersebut digunakan untuk mengidentifikasi kelas yang memiliki distribusi data sangat kecil. Kelas yang memiliki nilai prevalence ratio di bawah threshold sebesar 0.5% dari total data pelatihan dikategorikan sebagai kelas minoritas. Pada penelitian ini, jumlah data pada kelas minoritas tersebut kemudian ditingkatkan hingga 10 kali lipat melalui proses oversampling menggunakan SMOTE.

Untuk mengidentifikasi tingkat ketidakseimbangan distribusi data pada masing-masing kelas, dilakukan perhitungan class prevalence ratio pada data pelatihan. Rasio ini digunakan untuk mengukur proporsi setiap kelas terhadap keseluruhan data training sehingga dapat ditentukan kelas mana yang tergolong mayoritas dan minoritas. Hasil perhitungan tersebut disajikan pada Tabel 3.

Tabel 3. Kelas Prevalence Ratio Pada Data Pelatihan

Kelas	Data Training	Prevalence Ratio	Status
Normal	43099	53.46%	Mayoritas
DoS	29393	36.46%	Mayoritas
Probe	7460	9.25%	Mayoritas
R2L	637	0.79%	Minortitas
U2R	33	0.04%	Minortitas

Berdasarkan hasil perhitungan class prevalence ratio pada Tabel 3, dapat dilihat bahwa kelas U2R memiliki nilai prevalence ratio sebesar 0,04%, sedangkan kelas R2L memiliki nilai 0,79%. Berdasarkan threshold yang digunakan dalam penelitian ini yaitu 0,5%, kelas yang berada di bawah nilai threshold dikategorikan sebagai kelas minoritas yang memerlukan proses oversampling. Oleh karena itu, proses Selective SMOTE diterapkan pada kelas yang memenuhi kriteria tersebut untuk meningkatkan representasi data pada kelas minoritas. Penerapan SMOTE dilakukan hanya pada data pelatihan (training data) setelah proses pembagian dataset dilakukan. Pendekatan ini bertujuan untuk menghindari data leakage, sehingga data validasi dan data pengujian tetap menggunakan distribusi data asli. Selain itu, oversampling dilakukan secara terbatas agar tidak menyebabkan overfitting akibat dominasi data sintetis dalam proses pelatihan model. Dengan demikian, penerapan SMOTE dalam penelitian ini diharapkan dapat meningkatkan keseimbangan distribusi data pelatihan sehingga model CNN-LSTM mampu menghasilkan performa deteksi yang lebih baik, terutama dalam meningkatkan sensitivity (recall) terhadap serangan minoritas tanpa menurunkan specificity secara signifikan.

2.6 Pemodelan CNN-LSTM

Pada penelitian ini, model deteksi intrusi dibangun menggunakan arsitektur hybrid CNN–LSTM. Model ini dirancang untuk mengklasifikasikan data jaringan ke dalam lima kelas, yaitu Normal, DoS, Probe, R2L, dan U2R. Pemilihan arsitektur CNN–LSTM didasarkan pada kemampuannya dalam mengekstraksi pola lokal melalui lapisan konvolusi dan mempelajari hubungan antarf fitur melalui lapisan Long Short-Term Memory (LSTM) [13].

Sebelum data dimasukkan ke dalam model, data hasil preprocessing terlebih dahulu diubah bentuknya dari data tabular menjadi pseudo-sequence. Proses ini dilakukan dengan mereshape data menjadi format tiga dimensi dengan ukuran (jumlah sampel, jumlah fitur, 1). Dengan demikian, setiap sampel direpresentasikan sebagai urutan fitur yang dapat diproses oleh lapisan Conv1D dan LSTM. Selain itu, label target pada data latih dan data validasi dikonversi ke dalam bentuk one-hot encoding agar sesuai dengan kebutuhan klasifikasi multikelas menggunakan fungsi aktivasi softmax. Arsitektur model dimulai dengan lapisan input yang menerima data berdimensi (N_FEATURES, 1). Lapisan berikutnya adalah Conv1D pertama dengan 32 filter dan kernel size 3 serta fungsi aktivasi ReLU. Lapisan ini bertujuan untuk mengekstraksi pola lokal dari urutan fitur input. Keluaran dari lapisan konvolusi kemudian diproses menggunakan

JURIKOM (Jurnal Riset Komputer), Vol. 13 No. 2, April 2026
e-ISSN 2715-7393 (Media Online), p-ISSN 2407-389X (Media Cetak)
DOI 10.30865/jurikom.v13i2.9662
Hal 513-525
https://ejurnal.stmik-budidarma.ac.id/index.php/jurikom

Batch Normalization untuk menstabilkan distribusi aktivasi, dilanjutkan dengan MaxPooling1D berukuran 2 untuk mengurangi dimensi fitur, serta Dropout sebesar 0,2 untuk mengurangi risiko overfitting[17].

Tahap berikutnya adalah Conv1D kedua yang juga menggunakan 32 filter dan kernel size 3 dengan aktivasi ReLU. Sama seperti lapisan sebelumnya, keluaran dari lapisan ini dilanjutkan ke Batch Normalization, MaxPooling1D, dan Dropout 0,2. Penggunaan dua lapisan konvolusi bertujuan untuk memperkaya representasi fitur yang dipelajari dari data jaringan sebelum diteruskan ke lapisan sekuensial. Setelah proses ekstraksi fitur oleh CNN, keluaran model diteruskan ke lapisan LSTM dengan 64 unit dan parameter return_sequences=False. Lapisan ini berfungsi untuk mempelajari keterkaitan antarf fitur hasil ekstraksi konvolusi dan menghasilkan representasi akhir yang lebih informatif untuk proses klasifikasi. Selanjutnya, keluaran dari LSTM diteruskan ke Dense layer dengan 64 unit dan fungsi aktivasi ReLU. Pada lapisan ini diterapkan Dropout sebesar 0,4 untuk membantu mengurangi overfitting. Pada tahap akhir, model menggunakan Dense output layer dengan jumlah neuron sesuai banyaknya kelas dan fungsi aktivasi softmax untuk menghasilkan probabilitas klasifikasi pada setiap kelas[18].

Model dikompilasi menggunakan optimizer Adam dengan learning rate 0,001, fungsi loss categorical crossentropy, dan metrik evaluasi accuracy. Konfigurasi ini digunakan untuk mendukung proses pelatihan model klasifikasi multikelas secara stabil dan efisien. Secara umum, arsitektur CNN–LSTM pada penelitian ini dirancang untuk memanfaatkan kemampuan Conv1D dalam mengekstraksi pola fitur lokal dari data jaringan yang telah diubah menjadi pseudo-sequence, serta kemampuan LSTM dalam mempelajari representasi sekuensial dari fitur hasil ekstraksi. Dengan konfigurasi tersebut, model diharapkan mampu mengenali pola intrusi jaringan secara lebih efektif pada dataset NSL-KDD.

2.7 Desain Eksperimen dan Skenario Pengujian

Desain eksperimen dalam penelitian ini bertujuan untuk mengevaluasi pengaruh penerapan teknik Synthetic Minority Oversampling Technique (SMOTE) terhadap kinerja model CNN-LSTM dalam mendeteksi serangan jaringan. Eksperimen dilakukan dengan membandingkan performa model pada dua skenario utama, yaitu model tanpa penanganan ketidakseimbangan data (baseline) dan model yang menggunakan teknik SMOTE pada data pelatihan.

Pada skenario pertama, model CNN-LSTM baseline dilatih menggunakan dataset hasil preprocessing tanpa penerapan teknik oversampling. Pada tahap ini, distribusi data pelatihan tetap mengikuti distribusi asli dataset NSL-KDD yang memiliki ketidakseimbangan kelas, di mana jumlah data pada kelas mayoritas jauh lebih besar dibandingkan kelas minoritas. Skenario ini digunakan sebagai baseline untuk mengetahui performa awal model dalam mendeteksi intrusi jaringan tanpa penanganan khusus terhadap imbalanced data.

Pada skenario kedua, model CNN-LSTM + SMOTE dilatih menggunakan dataset pelatihan yang telah melalui proses penyeimbangan data menggunakan metode SMOTE. Teknik SMOTE diterapkan secara selektif pada kelas minoritas yang memiliki nilai class prevalence ratio di bawah threshold 0,5%, dengan peningkatan jumlah data hingga 10 kali lipat. Tujuan dari skenario ini adalah untuk meningkatkan representasi data pada kelas minoritas sehingga model dapat mempelajari karakteristik serangan secara lebih baik.

Dalam kedua skenario tersebut, proses pelatihan model dilakukan menggunakan data pelatihan, sedangkan data validasi digunakan untuk memantau performa model selama proses training dan membantu mengurangi risiko overfitting. Setelah proses pelatihan selesai, model dievaluasi menggunakan data pengujian (testing data) yang tidak digunakan selama proses pelatihan. Pendekatan ini bertujuan untuk memastikan bahwa hasil evaluasi model merepresentasikan kemampuan generalisasi model terhadap data baru.

Kinerja model pada setiap skenario kemudian dibandingkan menggunakan beberapa metrik evaluasi, yaitu accuracy, precision, recall (sensitivity), specificity, F1-score, dan false positive rate (FPR). Dalam penelitian ini, perhatian utama difokuskan pada peningkatan nilai sensitivity untuk meningkatkan kemampuan model dalam mendeteksi serangan minoritas, serta menjaga nilai specificity agar sistem tidak menghasilkan alarm palsu yang berlebihan pada trafik normal.

Melalui desain eksperimen tersebut, penelitian ini bertujuan untuk menganalisis sejauh mana penerapan teknik SMOTE dapat meningkatkan performa model CNN-LSTM dalam mendeteksi intrusi jaringan, khususnya pada kelas serangan yang memiliki jumlah data sangat sedikit.

2.8 Evaluasi Model

Tahap evaluasi dan pengujian dilakukan untuk mengukur kinerja model CNN-LSTM dalam mendeteksi intrusi jaringan pada dataset NSL-KDD. Evaluasi dilakukan menggunakan data pengujian (testing data) yang tidak digunakan selama proses pelatihan model. Pendekatan ini bertujuan untuk memastikan bahwa hasil pengujian dapat menggambarkan kemampuan generalisasi model terhadap data baru.

Pengukuran performa model dilakukan menggunakan beberapa metrik evaluasi yang umum digunakan dalam penelitian Intrusion Detection System (IDS), yaitu accuracy, precision, recall (sensitivity), specificity, F1-score, dan false positive rate (FPR)[19]. Metrik-metrik tersebut dihitung berdasarkan nilai confusion matrix yang terdiri dari True Positive (TP), True Negative (TN), False Positive (FP), dan False Negative (FN).

a. Accuracy

   Akurasi model adalah ukuran seberapa akurat perkiraannya secara keseluruhan (positif dan negatif yang diidentifikasi secara akurat).

$$Accuracy = \frac{TP+TN}{TP+TN+FP+FN} \quad (3)$$

JURIKOM (Jurnal Riset Komputer), Vol. 13 No. 2, April 2026
e-ISSN 2715-7393 (Media Online), p-ISSN 2407-389X (Media Cetak)
DOI 10.30865/jurikom.v13i2.9662
Hal 513-525
https://ejurnal.stmik-budidarma.ac.id/index.php/jurikom

b. Precision
Akurasi model adalah ukuran seberapa akurat perkiraannya secara keseluruhan (positif dan negatif yang diidentifikasi secara akurat).

$$Precision = \frac{TP}{TP+FP} \quad (4)$$

c. Recall (Sensitivity)
Recall mengevaluasi kapasitas model untuk secara akurat membedakan kejadian positif dari semua kasus positif yang sebenarnya dalam kumpulan data.

$$Recall = \frac{TP}{TP + FN} \quad (5)$$

d. Specificity
Specificity mengukur kemampuan model dalam mengenali data normal secara benar dari seluruh data normal yang tersedia.

$$Specificity = \frac{TN}{TN + FP} \quad (6)$$

e. F1-Score
F1-score merupakan ukuran yang menggabungkan precision dan recall untuk memberikan gambaran keseimbangan performa model.

$$F1 = 2 \times \frac{Precision \times Recall}{Precision + Recall} \quad (7)$$

f. FPR (False Positive Rate)
FPR menilai proporsi data normal yang salah diklasifikasikan sebagai serangan. Nilai FPR rendah sangat diharapkan agar IDS tidak menghasilkan terlalu banyak alarm palsu.

$$FPR = \frac{FP}{FP + TN} \quad (8)$$

3. HASIL DAN PEMBAHASAN

Penelitian ini menyajikan hasil eksperimen serta pembahasan kinerja model Intrusion Detection System (IDS) berbasis CNN-LSTM pada dataset NSL-KDD. Eksperimen dilakukan untuk menganalisis pengaruh penerapan metode Selective SMOTE berbasis prevalence ratio dalam mengatasi ketidakseimbangan data pada kelas serangan minoritas. Model dilatih menggunakan data yang telah melalui proses preprocessing, termasuk transformasi fitur, normalisasi menggunakan StandardScaler, serta pembagian dataset menjadi data pelatihan, validasi, dan pengujian. Kinerja model kemudian dievaluasi menggunakan metrik accuracy, precision, recall (sensitivity), specificity, F1-score, dan false positive rate (FPR) untuk menilai kemampuan model dalam mendeteksi serangan jaringan secara akurat sekaligus mempertahankan tingkat kesalahan deteksi yang rendah pada trafik normal.

3.1 Implementasi Eksperimen

Pada penelitian ini dilakukan implementasi model Intrusion Detection System (IDS) menggunakan arsitektur CNN–LSTM untuk mendeteksi aktivitas intrusi pada jaringan komputer. Model dibangun menggunakan framework TensorFlow dan Keras dan dilatih menggunakan dataset NSL-KDD yang telah melalui proses preprocessing meliputi labeling[20], mapping attack classes, penghapusan atribut yang tidak relevan, encoding fitur kategorikal, normalisasi menggunakan StandardScaler, serta pembagian dataset menjadi data pelatihan, validasi, dan pengujian.

Data input yang awalnya berbentuk tabular kemudian diubah menjadi pseudo-sequence dengan melakukan reshaping ke dalam bentuk tiga dimensi sehingga dapat diproses oleh lapisan Conv1D dan LSTM pada arsitektur model. Proses pelatihan dilakukan menggunakan data pelatihan, sementara data validasi digunakan untuk memantau performa model selama proses training. Evaluasi akhir model dilakukan menggunakan data pengujian untuk mengukur kemampuan generalisasi model terhadap data yang belum pernah digunakan sebelumnya.

Eksperimen dilakukan pada dua skenario pengujian, yaitu CNN-LSTM baseline dan CNN-LSTM dengan penerapan Selective SMOTE. Pada model baseline, pelatihan dilakukan menggunakan distribusi data asli yang masih memiliki ketidakseimbangan kelas. Sedangkan pada model usulan, dilakukan proses oversampling menggunakan Selective SMOTE berbasis prevalence ratio untuk meningkatkan jumlah data pada kelas minoritas.

Hasil eksperimen kemudian dianalisis menggunakan beberapa metrik evaluasi, yaitu accuracy, precision, recall (sensitivity), specificity, F1-score, dan false positive rate (FPR). Evaluasi ini bertujuan untuk menilai kemampuan model dalam mendeteksi serangan jaringan secara akurat serta menganalisis pengaruh penerapan Selective SMOTE terhadap peningkatan sensitivity tanpa menurunkan specificity secara signifikan.

3.2 Prapemrosesan Data

Tahap prapemrosesan data dilakukan untuk menyiapkan dataset NSL-KDD agar dapat digunakan secara optimal dalam proses pemodelan. Proses ini diawali dengan transformasi label serangan ke dalam lima kelas utama, yaitu normal, dos,

JURIKOM (Jurnal Riset Komputer), Vol. 13 No. 2, April 2026
e-ISSN 2715-7393 (Media Online), p-ISSN 2407-389X (Media Cetak)
DOI 10.30865/jurikom.v13i2.9662
Hal 513-525
https://ejurnal.stmik-budidarma.ac.id/index.php/jurikom

probe, r2l, dan u2r. Label yang tidak termasuk dalam kategori tersebut diklasifikasikan sebagai other dan kemudian dihapus dari dataset untuk memastikan konsistensi skenario klasifikasi multikelas. Sebagai contoh, label serangan seperti neptune dipetakan ke dalam kelas DoS, sedangkan ipsweep masuk ke dalam kelas Probe, sehingga kompleksitas label yang semula beragam dapat disederhanakan menjadi lima kategori utama yang lebih representatif.

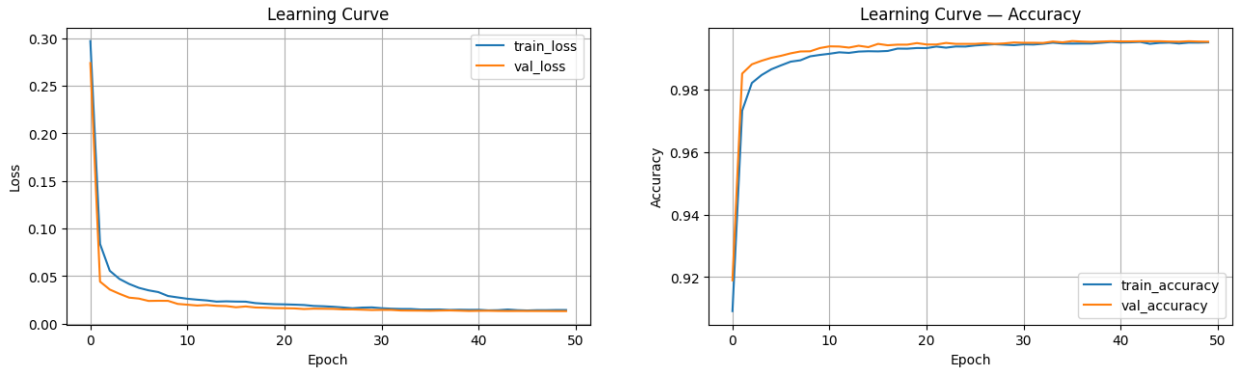
Selanjutnya, dilakukan pemisahan antara fitur input dan target dengan menghapus atribut yang tidak digunakan dalam pemodelan, yaitu label, difficulty, class, dan class_id, sehingga jumlah fitur berkurang dari 45 atribut awal menjadi 41 fitur utama sesuai standar dataset NSL-KDD. Fitur tersebut terdiri atas fitur kategorikal seperti protocol_type, service, dan flag, serta fitur numerik lainnya. Pada tahap transformasi data, fitur kategorikal dikonversi menggunakan One-Hot Encoding, misalnya nilai tcp direpresentasikan menjadi vektor biner (1,0,0). Selanjutnya, fitur numerik dinormalisasi menggunakan StandardScaler agar memiliki distribusi yang seragam, di mana nilai seperti src_bytes = 181 dapat berubah menjadi nilai terstandarisasi, misalnya -0,45, berdasarkan rata-rata dan deviasi standar data pelatihan. Proses fitting dilakukan hanya pada data pelatihan, kemudian transformasi yang sama diterapkan pada data validasi dan data pengujian untuk mencegah terjadinya data leakage.

Dataset kemudian dibagi menjadi tiga bagian, yaitu data pelatihan, validasi, dan pengujian. Pembagian dilakukan dengan skema 80:20 untuk data pelatihan dan pengujian, kemudian data pelatihan dibagi kembali 80:20 untuk menghasilkan data pelatihan dan validasi. Berdasarkan pembagian tersebut diperoleh 80.622 data pelatihan, 20.156 data validasi, dan 25.195 data pengujian. Hasil prapemrosesan menunjukkan bahwa data telah berhasil ditransformasikan ke dalam bentuk numerik dengan dimensi fitur yang sesuai untuk proses pemodelan. Selain itu, distribusi data antar kelas tetap mempertahankan karakteristik ketidakseimbangan awal yang kemudian ditangani menggunakan metode Selective SMOTE pada tahap selanjutnya.

3.3 Pemodelan CNN-LSTM

Pada tahap ini dilakukan implementasi model CNN–LSTM untuk mendeteksi aktivitas intrusi pada dataset NSL-KDD yang telah melalui proses prapemrosesan. Data yang telah ditransformasikan ke dalam bentuk numerik kemudian diubah menjadi pseudo-sequence dengan format tiga dimensi (jumlah sampel, jumlah fitur, 1) agar dapat diproses oleh lapisan Conv1D dan LSTM. Transformasi ini memungkinkan model untuk menangkap pola hubungan antar fitur secara lebih efektif, baik dalam konteks spasial maupun temporal.

Model CNN–LSTM dibangun menggunakan framework TensorFlow dan Keras dengan konfigurasi arsitektur yang telah ditentukan. Arsitektur model terdiri dari dua lapisan Conv1D dengan masing-masing 32 filter dan kernel size 3 yang menggunakan fungsi aktivasi ReLU. Setiap lapisan konvolusi diikuti oleh Batch Normalization, MaxPooling1D, dan Dropout sebesar 0,2 untuk meningkatkan stabilitas pelatihan serta mengurangi risiko overfitting. Selanjutnya, fitur hasil ekstraksi diteruskan ke lapisan LSTM dengan 64 unit untuk mempelajari hubungan antar fitur secara lebih mendalam. Pada bagian akhir model, digunakan Dense layer dengan 64 unit dan fungsi aktivasi ReLU, serta Dropout sebesar 0,4 sebelum masuk ke lapisan output dengan fungsi aktivasi softmax untuk menghasilkan probabilitas klasifikasi pada lima kelas. Model dikompilasi menggunakan optimizer Adam dengan learning rate sebesar 0,001 dan fungsi loss categorical crossentropy. Proses pelatihan model dilakukan selama maksimal 50 epoch dengan batch size 256, serta menggunakan mekanisme EarlyStopping dan ReduceLROnPlateau untuk menjaga stabilitas pelatihan[18][20].



Gambar 2. Kurva Training Loss dan Validation Baseline

Gambar 2. menunjukkan kurva learning curve berupa loss dan accuracy selama proses pelatihan. Terlihat bahwa nilai training loss mengalami penurunan yang signifikan dari sekitar 0,30 pada epoch awal hingga berada di bawah 0,02, sementara validation loss juga menunjukkan tren penurunan yang stabil dengan nilai yang relatif berdekatan. Hal ini menunjukkan bahwa model mampu melakukan pembelajaran secara efektif tanpa indikasi overfitting yang signifikan.

Pada sisi accuracy, nilai training accuracy meningkat secara cepat dari sekitar 91% hingga mencapai lebih dari 99%, diikuti oleh validation accuracy yang menunjukkan pola peningkatan yang konsisten dan berada pada kisaran yang

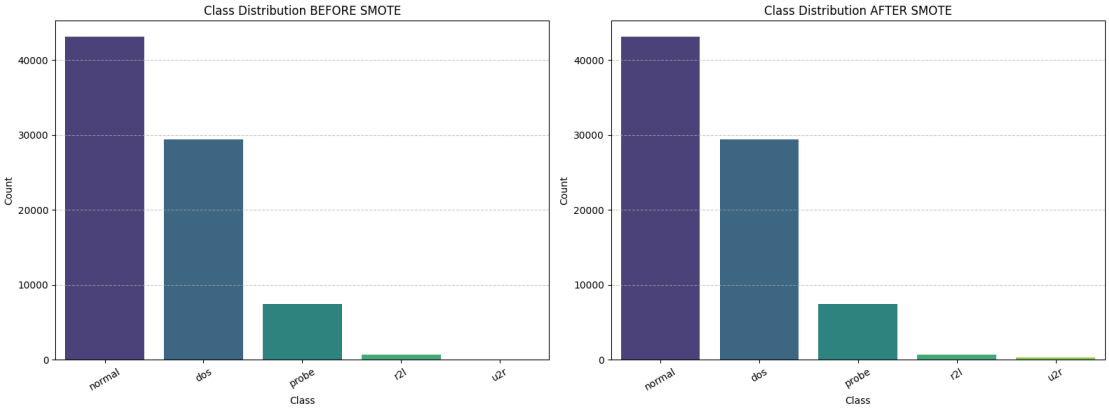
JURIKOM (Jurnal Riset Komputer), Vol. 13 No. 2, April 2026
e-ISSN 2715-7393 (Media Online), p-ISSN 2407-389X (Media Cetak)
DOI 10.30865/jurikom.v13i2.9662
Hal 513-525
https://ejurnal.stmik-budidarma.ac.id/index.php/jurikom

hampir sama. Kedekatan antara kurva pelatihan dan validasi menunjukkan bahwa model memiliki kemampuan generalisasi yang baik.

3.4 Penerapan Selective SMOTE (Synthetic Minority Oversampling Technique)

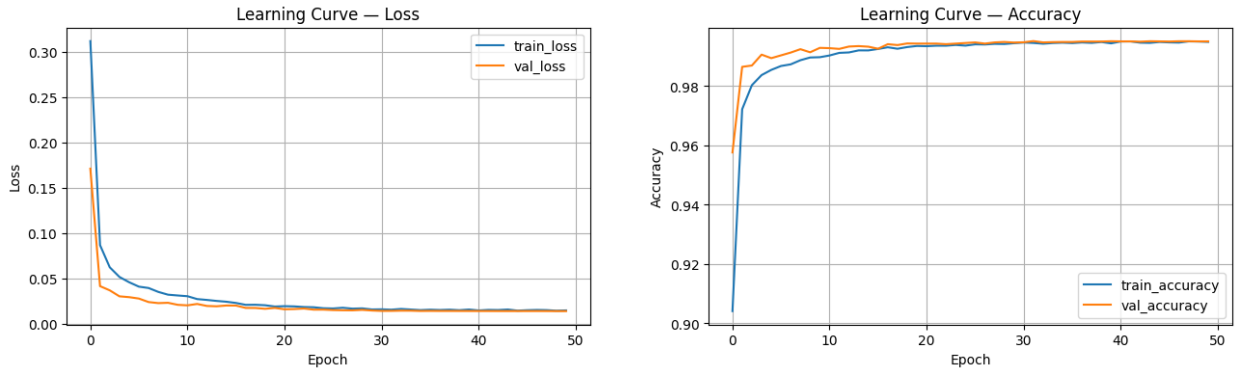
Pada tahap ini dilakukan penerapan metode Selective SMOTE (Synthetic Minority Oversampling Technique) untuk mengatasi permasalahan ketidakseimbangan data pada dataset NSL-KDD. Ketidakseimbangan data yang signifikan, khususnya pada kelas minoritas seperti R2L dan U2R, berpotensi menyebabkan model cenderung bias terhadap kelas mayoritas dan menurunkan kemampuan dalam mendeteksi serangan dengan frekuensi rendah. Oleh karena itu, diperlukan teknik penyeimbangan data yang mampu meningkatkan representasi kelas minoritas tanpa mengganggu distribusi asli secara berlebihan.

Berbeda dengan pendekatan SMOTE konvensional yang melakukan oversampling pada seluruh kelas minoritas, penelitian ini menerapkan Selective SMOTE berbasis prevalence ratio, di mana hanya kelas dengan proporsi di bawah threshold 0,5% yang akan dilakukan oversampling. Selain itu, jumlah data pada kelas tersebut ditingkatkan secara terbatas dengan faktor pengali tertentu (10×) untuk menghindari terjadinya overfitting akibat dominasi data sintetis.



Gambar 3. Distribusi Kelas Data Pelatihan Sebelum dan Sesudah SMOTE

Gambar 3 menunjukkan perbandingan distribusi kelas pada data pelatihan sebelum dan sesudah penerapan metode Selective SMOTE. Pada kondisi sebelum SMOTE, distribusi data terlihat sangat tidak seimbang, di mana kelas normal memiliki 43.099 data (53.46%) dan kelas DoS sebanyak 29.393 data (36.46%), sehingga mendominasi dataset. Sementara itu, kelas Probe hanya memiliki 7.460 data (9.25%), kelas R2L sebanyak 637 data (0.79%), dan kelas U2R hanya 33 data (0.04%), yang menunjukkan ketimpangan yang sangat signifikan pada kelas minoritas. Setelah penerapan SMOTE, jumlah data pada kelas tersebut meningkat menjadi sekitar 330 data, sehingga distribusi menjadi lebih representatif. Sementara itu, kelas lainnya seperti normal, DoS, Probe, dan R2L tidak mengalami perubahan jumlah data karena tidak berada di bawah threshold 0.5% yang ditetapkan dalam penelitian ini.



Gambar 4. Kurva Training Loss dan Validation Selective Smote

Setelah proses penyeimbangan data dilakukan, model CNN–LSTM dilatih kembali menggunakan dataset hasil SMOTE dengan konfigurasi arsitektur yang sama seperti pada model baseline. Gambar 4. menunjukkan kurva learning curve berupa loss dan accuracy selama proses pelatihan model dengan SMOTE. Terlihat bahwa nilai training loss mengalami penurunan yang signifikan dari sekitar 0,31 hingga di bawah 0,02, sedangkan validation loss juga menunjukkan tren penurunan yang stabil. Pada kurva accuracy, nilai training accuracy meningkat dari sekitar 90% menjadi lebih dari 99%, dan diikuti oleh validation accuracy yang berada pada kisaran yang sama. Kedekatan antara kurva pelatihan dan validasi menunjukkan bahwa model tetap memiliki kemampuan generalisasi yang baik serta tidak mengalami overfitting meskipun jumlah data pada kelas minoritas telah ditingkatkan.

JURIKOM (Jurnal Riset Komputer), Vol. 13 No. 2, April 2026
e-ISSN 2715-7393 (Media Online), p-ISSN 2407-389X (Media Cetak)
DOI 10.30865/jurikom.v13i2.9662
Hal 513-525
https://ejurnal.stmik-budidarma.ac.id/index.php/jurikom

Hasil ini menunjukkan bahwa penerapan Selective SMOTE berhasil meningkatkan distribusi data pada kelas yang sangat minoritas tanpa mengubah distribusi kelas mayoritas secara signifikan. Pendekatan ini memungkinkan model untuk memperoleh informasi yang lebih representatif pada kelas minoritas, khususnya U2R, sehingga diharapkan dapat meningkatkan kemampuan model dalam mendeteksi serangan pada kelas tersebut, terutama dalam hal peningkatan nilai sensitivity (recall), tanpa menyebabkan peningkatan false positive rate yang signifikan pada kelas normal.

3.5 Hasil Evaluasi Model

Pada tahap ini dilakukan evaluasi performa model untuk membandingkan kinerja antara CNN–LSTM baseline dan CNN–LSTM dengan Selective SMOTE. Evaluasi dilakukan menggunakan data uji yang tidak terlibat dalam proses pelatihan, dengan metrik meliputi accuracy, precision, recall (sensitivity), specificity, F1-score, serta false positive rate (FPR).

Tabel 4. Metrik Evaluasi CNN-LSTM Baseline Dengan SMOTE

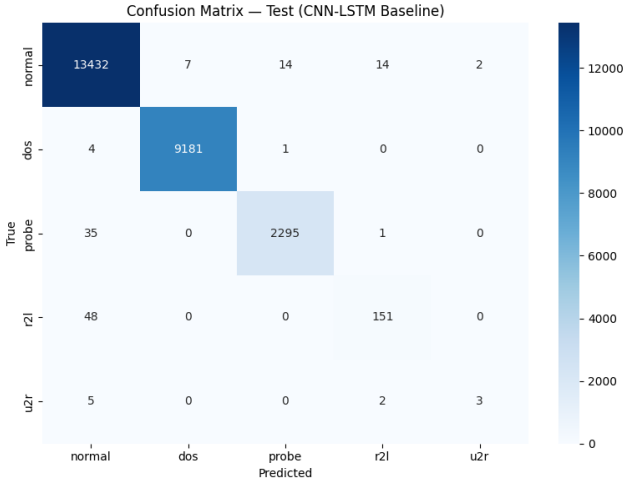
Model	Metode Resampling	Metrik Evaluasi					
		Accuracy	Precision	Recall	Specificity	F1-Score	FPR
CNN-LSTM	-	0.9947	0.897	0.808	0.9981	0.8413	0.0078
	SMOTE	0.9946	0.8437	0.8929	0.9981	0.8515	0.0072

Berdasarkan Tabel 4. kedua model menunjukkan nilai accuracy yang sangat tinggi (≈99%), sehingga perbedaan performa tidak terlihat signifikan pada metrik ini. Namun, peningkatan yang jelas terlihat pada recall (sensitivity) dan F1-score, di mana model dengan Selective SMOTE meningkatkan recall dari 0.8080 menjadi 0.8929. Peningkatan ini menunjukkan bahwa model menjadi lebih mampu mendeteksi serangan, khususnya pada kelas minoritas.

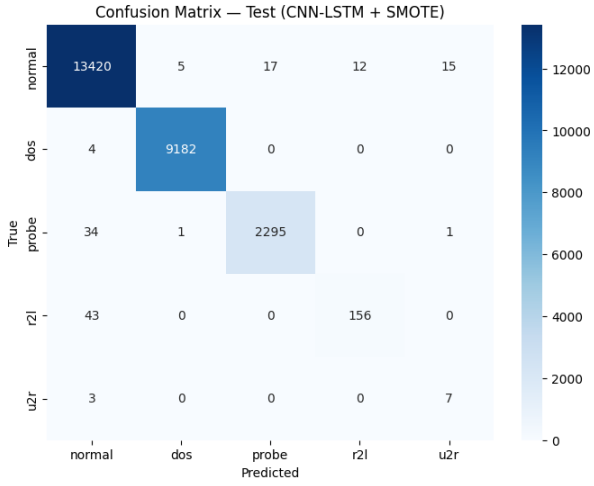
Tabel 5. Metrik Evaluasi CNN-LSTM Baseline Dengan SMOTE

Kelas	CNN-LSTM Baseline			CNN-LSTM + SMOTE		
	Precision	Recall	F1	Precision	Recall	F1
Normal	0.9932	0.9973	0.9952	0.9938	0.9964	0.9951
DoS	0.9992	0.9995	0.9993	0.9993	0.9996	0.9995
Probe	0.9935	0.9846	0.989	0.9926	0.9846	0.9886
R2L	0.8988	0.7588	0.8229	0.9286	0.7839	0.8501
U2R	0.6	0.3	0.4	0.3043	0.7	0.4242

Pada Tabel 5. menunjukkan bahwa performa pada kelas mayoritas relatif stabil, sedangkan peningkatan signifikan terjadi pada kelas minoritas. Pada kelas U2R, recall meningkat drastis dari 0.3000 menjadi 0.7000, sementara kelas R2L meningkat dari 0.7588 menjadi 0.7839. Hal ini menunjukkan bahwa Selective SMOTE efektif dalam meningkatkan kemampuan deteksi terhadap serangan langka.



Gambar 5. Confution Matrix CNN-LSTM Baseline



Gambar 6. Confution Matrix CNN-LSTM + SMOTE

Confusion matrix pada Gambar 5 Dan gambar 6 menunjukkan bahwa pada model baseline masih terdapat kesalahan klasifikasi yang cukup tinggi pada kelas minoritas, khususnya U2R dan R2L, di mana sebagian besar data salah diklasifikasikan sebagai kelas lain. Setelah penerapan Selective SMOTE, jumlah prediksi yang benar pada kelas minoritas meningkat, yang ditunjukkan dengan bertambahnya nilai diagonal pada confusion matrix. Hal ini mengindikasikan peningkatan kemampuan model dalam mengenali pola serangan yang sebelumnya kurang terwakili.

JURIKOM (Jurnal Riset Komputer), Vol. 13 No. 2, April 2026
e-ISSN 2715-7393 (Media Online), p-ISSN 2407-389X (Media Cetak)
DOI 10.30865/jurikom.v13i2.9662
Hal 513-525
https://ejurnal.stmik-budidarma.ac.id/index.php/jurikom

3.6 Pembahasan

Hasil penelitian menunjukkan bahwa model CNN–LSTM baseline telah mampu menghasilkan performa yang sangat tinggi dari sisi accuracy, yaitu di atas 99%. Hal ini menunjukkan bahwa arsitektur CNN–LSTM efektif dalam menangkap pola karakteristik data jaringan pada dataset NSL-KDD. Lapisan Conv1D mampu mengekstraksi pola lokal antar fitur, sementara lapisan LSTM berperan dalam menangkap hubungan dependensi antar fitur secara lebih kompleks. Namun demikian, performa tinggi pada accuracy tidak sepenuhnya mencerminkan kemampuan model dalam mendeteksi seluruh jenis serangan, terutama pada kondisi data yang tidak seimbang.

Permasalahan utama yang ditemukan pada model baseline adalah rendahnya kemampuan dalam mendeteksi kelas minoritas, khususnya U2R dan R2L. Hal ini ditunjukkan oleh nilai recall yang rendah, yaitu sebesar 0,30 untuk U2R dan 0,7588 untuk R2L pada data uji. Kondisi ini mengindikasikan bahwa model cenderung bias terhadap kelas mayoritas seperti normal dan DoS, yang memiliki jumlah data jauh lebih besar. Fenomena ini umum terjadi pada dataset imbalanced, di mana model lebih mengoptimalkan prediksi pada kelas dominan sehingga mengabaikan pola pada kelas minoritas. Untuk mengatasi permasalahan tersebut, penelitian ini mengusulkan pendekatan Selective SMOTE berbasis prevalence ratio, yang hanya melakukan oversampling pada kelas dengan proporsi sangat kecil. Berbeda dengan SMOTE konvensional yang menyeimbangkan seluruh kelas secara agresif, pendekatan ini lebih selektif sehingga mampu menjaga distribusi data tetap realistis dan menghindari risiko overfitting. Selain itu, penerapan SMOTE hanya pada data pelatihan juga memastikan tidak terjadinya data leakage, sehingga hasil evaluasi tetap valid.

Hasil eksperimen menunjukkan bahwa penerapan Selective SMOTE memberikan peningkatan signifikan pada kemampuan deteksi kelas minoritas. Nilai recall pada kelas U2R meningkat secara drastis dari 0.30 menjadi 0.70, sedangkan kelas R2L meningkat dari 0.7588 menjadi 0.7839. Secara keseluruhan, nilai macro recall meningkat dari 0,808 menjadi 0.8929, yang menunjukkan peningkatan sensitivitas model dalam mendeteksi berbagai jenis serangan. Hal ini menjadi indikator utama bahwa metode yang diusulkan berhasil mengatasi permasalahan ketidakseimbangan data. Meskipun terjadi penurunan pada nilai precision macro, hal ini merupakan trade-off yang umum dalam peningkatan recall, terutama pada konteks deteksi intrusi. Dalam sistem IDS, peningkatan kemampuan mendeteksi serangan (high recall) seringkali lebih diprioritaskan dibandingkan dengan sedikit peningkatan false alarm. Hal ini dikarenakan kegagalan mendeteksi serangan (false negative) memiliki dampak yang jauh lebih kritis dibandingkan kesalahan deteksi (false positive). Selain itu, hasil penelitian juga menunjukkan bahwa nilai specificity tetap stabil (≈0,9981) dan false positive rate (FPR) tetap rendah, bahkan mengalami sedikit penurunan setelah penerapan SMOTE. Hal ini menunjukkan bahwa peningkatan sensitivitas terhadap kelas minoritas tidak mengorbankan kemampuan model dalam mengenali trafik normal. Dengan demikian, model yang diusulkan mampu mencapai keseimbangan yang optimal antara sensitivity dan specificity, yang merupakan aspek penting dalam sistem IDS.

Secara keseluruhan, hasil penelitian ini menunjukkan bahwa pendekatan Selective SMOTE berbasis prevalence ratio mampu meningkatkan performa model secara signifikan pada aspek yang paling krusial, yaitu deteksi serangan minoritas, tanpa menurunkan stabilitas model secara keseluruhan. Oleh karena itu, metode yang diusulkan memiliki potensi untuk diterapkan dalam sistem deteksi intrusi nyata yang membutuhkan tingkat akurasi tinggi sekaligus kemampuan deteksi yang sensitif terhadap berbagai jenis serangan.

4. KESIMPULAN

Berdasarkan hasil penelitian yang telah dilakukan, dapat disimpulkan bahwa model CNN–LSTM mampu memberikan performa yang sangat baik dalam mendeteksi intrusi pada dataset NSL-KDD, yang ditunjukkan oleh nilai accuracy di atas 99%, sehingga membuktikan efektivitas arsitektur dalam menangkap pola data jaringan. Namun demikian, model baseline masih menunjukkan keterbatasan dalam mendeteksi kelas minoritas seperti U2R dan R2L, yang disebabkan oleh ketidakseimbangan distribusi data sehingga model cenderung bias terhadap kelas mayoritas. Untuk mengatasi permasalahan tersebut, penelitian ini mengusulkan metode Selective SMOTE berbasis prevalence ratio, yang secara selektif melakukan oversampling pada kelas dengan proporsi sangat kecil. Hasil eksperimen menunjukkan bahwa pendekatan ini mampu meningkatkan nilai recall secara signifikan, khususnya pada kelas minoritas, tanpa menurunkan nilai specificity maupun meningkatkan false positive rate secara berarti, sehingga menghasilkan keseimbangan performa yang lebih optimal. Meskipun demikian, penelitian ini masih memiliki keterbatasan, antara lain penggunaan satu dataset serta penentuan parameter SMOTE yang masih bersifat empiris. Oleh karena itu, penelitian selanjutnya disarankan untuk menguji metode pada dataset lain serta mengembangkan pendekatan yang lebih adaptif guna meningkatkan generalisasi model.

REFERENCES

[1] H. Nandanwar and R. Katarya, “Securing Industry 5.0: An explainable deep learning model for intrusion detection in cyber-physical systems,” *Comput. Electr. Eng.*, vol. 123, no. PC, p. 110161, 2025, doi: 10.1016/j.compeleceng.2025.110161.

[2] L. Wu, Y. Xie, J. Li, D. Feng, J. Liang, and Y. Wu, “Angus: efficient active learning strategies for provenance based intrusion detection,” *Cybersecurity*, vol. 8, no. 1, 2025, doi: 10.1186/s42400-024-00311-y.

[3] S. H. Mohammed *et al.*, *Dual-hybrid intrusion detection system to detect False Data Injection in smart grids*, vol. 20, no. 1

January. 2025. doi: 10.1371/journal.pone.0316536.

[4] A. Halbouni, T. S. Gunawan, M. H. Habaebi, M. Halbouni, M. Kartiwi, and R. Ahmad, "CNN-LSTM: Hybrid Deep Neural Network for Network Intrusion Detection System," *IEEE Access*, vol. 10, pp. 99837–99849, 2022, doi: 10.1109/ACCESS.2022.3206425.

[5] P. Ananthi, K. Nirmaladevi, and S. Naveen Kumar, "Intrusion Detection Mechanism Using Deep Learning," *Proc. 5th Int. Conf. IoT Based Control Networks Intell. Syst. ICICNIS 2024*, pp. 188–194, 2024, doi: 10.1109/ICICNIS64247.2024.10823331.

[6] D. Elreedy, A. F. Atiya, and F. Kamalov, "A theoretical distribution analysis of synthetic minority oversampling technique (SMOTE) for imbalanced learning," *Mach. Learn.*, vol. 113, no. 7, pp. 4903–4923, 2024, doi: 10.1007/s10994-022-06296-4.

[7] R. A. Disha and S. Waheed, "Performance analysis of machine learning models for intrusion detection system using Gini Impurity-based Weighted Random Forest (GIWRF) feature selection technique," *Cybersecurity*, vol. 5, no. 1, pp. 1–22, 2022, doi: 10.1186/s42400-021-00103-8.

[8] Z. Wang, Y. Zhou, T. Takagi, J. Song, Y. S. Tian, and T. Shibuya, "Genetic algorithm-based feature selection with manifold learning for cancer classification using microarray data," *BMC Bioinformatics*, vol. 24, no. 1, pp. 1–22, 2023, doi: 10.1186/s12859-023-05267-3.

[9] M. B. Umair, Z. Iqbal, M. A. Faraz, and M. A. Khan, "A Network Intrusion Detection System Using Hybrid Multilayer Deep Learning Model," vol. 12, no. 5, pp. 367–376, 2024, doi: 10.1089/big.2021.0268.

[10] V. Mansotra, A. Mahajan, and K. Singh, "Hybrid CNN-LSTM Model Combined with Feature Selection and SMOTE for Detection of Network Attacks," *Int. J. Sens. Networks*, vol. 43, no. 4, 2023, doi: 10.1504/ijsnet.2023.10060962.

[11] V. Hnamte, H. Nhung-Nguyen, J. Hussain, and Y. Hwa-Kim, "A Novel Two-Stage Deep Learning Model for Network Intrusion Detection: LSTM-AE," *IEEE Access*, vol. 11, pp. 37131–37148, 2023, doi: 10.1109/ACCESS.2023.3266979.

[12] N. Hussen, S. M. Elghamrawy, M. Salem, and A. I. El-Desouky, "A Fully Streaming Big Data Framework for Cyber Security Based on Optimized Deep Learning Algorithm," *IEEE Access*, vol. 11, pp. 65675–65688, 2023, doi: 10.1109/ACCESS.2023.3281893.

[13] H. Yu, C. Kang, Y. Xiao, and Y. Yang, "Network Intrusion Detection Method Based on Hybrid Improved Residual Network Blocks and Bidirectional Gated Recurrent Units," *IEEE Access*, vol. 11, pp. 68961–68971, 2023, doi: 10.1109/ACCESS.2023.3271866.

[14] N. Zhu, G. Zhao, Y. Yang, H. Yang, and Z. Liu, "AEC_GAN: Unbalanced Data Processing Decision-Making in Network Attacks Based on ACGAN and Machine Learning," *IEEE Access*, vol. 11, no. May, pp. 52452–52465, 2023, doi: 10.1109/ACCESS.2023.3280421.

[15] S. Montaha, S. Azam, A. K. M. R. H. Rafid, M. Z. Hasan, A. Karim, and A. Islam, "TimeDistributed-CNN-LSTM: A Hybrid Approach Combining CNN and LSTM to Classify Brain Tumor on 3D MRI Scans Performing Ablation Study," *IEEE Access*, vol. 10, pp. 60039–60059, 2022, doi: 10.1109/ACCESS.2022.3179577.

[16] S. Prasath, K. Sethi, D. Mohanty, P. Bera, and S. R. Samantaray, "Analysis of Continual Learning Models for Intrusion Detection System," *IEEE Access*, vol. 10, pp. 121444–121464, 2022, doi: 10.1109/ACCESS.2022.3222715.

[17] S. Suman *et al.*, "Attention Based CNN-LSTM Network for Pulmonary Embolism Prediction on Chest Computed Tomography Pulmonary Angiograms," *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 12907 LNCS, pp. 356–366, 2021, doi: 10.1007/978-3-030-87234-2_34.

[18] Ian Goodfellow and Yoshua Bengio and Aaron Courville, *Deep Learning*. MIT Press, 2016. [Online]. Available: http://www.deeplearningbook.org

[19] C. Wang, X. Wang, X. Jing, H. Yokoi, W. Huang, and M. Zhu, "Towards high-accuracy classifying attention- deficit / hyperactivity disorders using CNN-LSTM model Towards high-accuracy classifying attention-deficit / hyperactivity disorders using CNN-LSTM model," 2022.

[20] A. Géron, *Hands-On Machine Learning with Scikit-Learn, Keras, and TensorFlow: Concepts, Tools, and Techniques to Build Intelligent Systems*. O'Reilly Media, 2019. [Online]. Available: https://books.google.co.id/books?id=HHetDwAAQBAJ