Jurnal Riset Sistem Informasi Dan Teknik Informatika (JURASIK)
Volume 10, Nomor 2, Agustus 2025, pp 528-539
Terakreditasi Nomor 204/E/KPT/2022 | ISSN: 2527-5771/EISSN: 2549-7839
https://tunasbangsa.ac.id/ejurnal/index.php/jurasik

Peningkatan Akurasi Deteksi Intrusi Jaringan dengan Model Hybrid Convolutional Neural Network dan Long Short-Term Memory

Ficho Pranandasya Andrian Pratama[1], Danang Arbian Sulistyo[2], Fransiska Sisilia Mukti[3]
[1,2,3]Institut Teknologi dan Bisnis Asia Malang, Indonesia
Email: rkyouya0@gmail.com[1], danangarbian@gmail.com[2], ms.frans@asia.ac.id[3]

Abstract

The evolving cyber threats demand more sophisticated and accurate intrusion detection systems (IDS). This research develops a hybrid CNN-LSTM model with comprehensive data preprocessing techniques to enhance network attack detection accuracy. The UNSW-NB15 dataset consisting of nine attack categories and 49 features was used as research data. The methodology begins with data preprocessing including data cleaning, categorical transformation using categorical codes, class balancing with upsampling, StandardScaler normalization, and 80:20 data splitting. The hybrid model architecture combines three CNN blocks for spatial feature extraction with two LSTM layers for modeling temporal dependencies. The model was compiled using Adam optimizer with 0.0005 learning rate and equipped with EarlyStopping, ReduceLROnPlateau, and ModelCheckpoint callbacks. Evaluation results show the CNN-LSTM model achieves 99% accuracy, precision, recall, and F1-score, significantly outperforming the standard CNN model which only reaches 96%. Learning curves demonstrate rapid convergence without overfitting indication. This research proves that the combination of CNN's spatial feature extraction capability and LSTM's temporal dependency modeling is highly effective for anomaly detection in complex sequential data such as network traffic.

Keywords*: deep learning, CNN-LSTM, Intrusion Detection System, network security, UNSW-NB15*

Abstrak

Ancaman siber yang terus berkembang menuntut sistem deteksi intrusi (IDS) yang lebih canggih dan akurat. Penelitian ini mengembangkan model hybrid CNN-LSTM dengan teknik pra-pemrosesan komprehensif untuk meningkatkan akurasi deteksi serangan jaringan. Dataset UNSW-NB15 yang terdiri dari sembilan kategori serangan dan 49 fitur digunakan sebagai data penelitian. Metodologi dimulai dengan pra-pemrosesan data meliputi pembersihan data, transformasi kategorikal menggunakan categorical codes, penyeimbangan kelas dengan upsampling, normalisasi StandardScaler, dan pembagian data 80:20. Arsitektur model hybrid menggabungkan tiga blok CNN untuk ekstraksi fitur spasial dengan dua lapisan LSTM untuk memodelkan dependensi temporal. Model dikompilasi menggunakan optimizer Adam dengan learning rate 0.0005 dan dilengkapi callback EarlyStopping, ReduceLROnPlateau, dan ModelCheckpoint. Hasil evaluasi menunjukkan model CNN-LSTM mencapai akurasi, presisi, recall, dan F1-score 99%, unggul signifikan dibandingkan model CNN standar yang hanya mencapai 96%. Kurva pembelajaran menunjukkan konvergensi cepat tanpa indikasi overfitting. Penelitian ini membuktikan bahwa kombinasi kemampuan CNN dalam ekstraksi fitur spasial dan LSTM dalam memodelkan dependensi temporal sangat efektif untuk deteksi anomali pada data sekuensial kompleks seperti lalu lintas jaringan.

Kata kunci*: deep learning, CNN-LSTM, Sistem Deteksi Intrusi, keamanan jaringan, UNSW-NB15*

1. PENDAHULUAN

Dalam era digital yang berkembang pesat, keamanan jaringan menjadi aspek penting bagi organisasi dan individu yang bergantung pada infrastruktur jaringan untuk mengakses dan mengelola informasi. Serangan siber yang terus meningkat,

seperti DDoS, malware, dan serangan *zero-day*, menuntut sistem deteksi intrusi (IDS) yang lebih canggih dan akurat untuk menjaga keamanan jaringan. Keamanan jaringan mencakup perlindungan data dari akses yang tidak sah, perlindungan terhadap kerusakan data, dan implementasi kebijakan untuk pemulihan dari pelanggaran keamanan serta kehilangan data. Aspek penting keamanan jaringan adalah menjaga kerahasiaan, integritas, dan ketersediaan informasi yang melekat pada sistem [1].

Dalam upaya mendeteksi serangan jaringan, evolusi *Intrusion Detection System* (IDS) telah bergeser signifikan dari metode konvensional seperti deteksi berbasis tanda tangan (*signature-based detection*), yang efektif untuk serangan yang dikenal tetapi tidak mampu mendeteksi serangan *zero-day* atau pola baru akibat volume data besar dan teknik *evasion* canggih, menuju pendekatan berbasis pembelajaran mesin (*machine learning based*) yang lebih canggih. Pendekatan machine learning, khususnya deep learning, memungkinkan IDS untuk mengidentifikasi aktivitas mencurigakan dengan mempelajari pola perilaku normal dan menandai penyimpangan sebagai anomali, sehingga lebih efektif dalam mendeteksi serangan baru atau zero-day. Pemanfaatan analitik canggih berbasis AI/ML ini mendukung analisis real-time dan prediktif, serta pembuatan profil perilaku yang lebih mendalam, menjadikannya solusi relevan untuk tantangan keamanan siber modern. Metode konvensional IDS sering kali tidak mampu mendeteksi serangan baru secara efektif, sehingga teknologi deep learning semakin diminati sebagai solusi yang dapat belajar dari pola data yang kompleks. Teknik machine learning (ML) telah menjadi sangat penting dalam analisis lalu lintas jaringan karena kemampuannya menangani kompleksitas dan keragaman aliran data modern. Berbeda dengan metode statistik tradisional yang sering kesulitan menangkap pola dan anomali dalam jaringan berskala besar dan dinamis, model ML unggul dalam mempelajari data dalam jumlah besar serta mengidentifikasi hubungan yang rumit [2].

Algoritma deep learning telah terbukti signifikan dalam pengenalan suara, pemrosesan gambar, pemrosesan bahasa alami, dan banyak domain lainnya. Penelitian ini berfokus pada efektivitas arsitektur deep learning untuk solusi keamanan jaringan yang memindai lalu lintas jaringan untuk mengidentifikasi dan melaporkan pelanggaran berdasarkan fitur perilaku intrusi [3]. Dalam ranah IDS, baik machine learning maupun deep learning telah diadopsi untuk meningkatkan kemampuan deteksi serangan, meskipun keduanya memiliki perbedaan fundamental dalam pendekatannya. Deep learning adalah pendekatan yang menjanjikan untuk mengembangkan sistem deteksi intrusi (IDS) yang fleksibel dan efektif dalam mendeteksi serangan siber yang tidak terduga. Model hybrid yang menggabungkan pendekatan berbasis jaringan (NIDS) dan berbasis host (HIDS) dapat meningkatkan akurasi deteksi serangan dengan memanfaatkan representasi fitur yang hierarkis dan dinamis [4]. Deep learning adalah paradigma baru dalam bidang machine learning yang terutama dibangun menggunakan ANN (*artificial neural networks*) dan memiliki kinerja lebih tinggi dibandingkan teknik machine learning konvensional lainnya [5]. Machine learning (ML) tradisional dalam IDS umumnya memerlukan rekayasa fitur (*feature engineering*) secara manual, di

mana para ahli domain harus secara eksplisit mendefinisikan dan mengekstrak fitur-fitur relevan dari data lalu lintas jaringan yang kemudian digunakan oleh algoritma ML (seperti *Support Vector Machine*, *Decision Tree*, atau *Random Forest*) untuk mengklasifikasikan aktivitas sebagai normal atau mencurigakan. Meskipun efektif untuk pola serangan yang jelas dan fitur yang terdefinisi dengan baik, kinerja model ML dapat sangat bergantung pada kualitas dan kelengkapan proses rekayasa fitur ini. Sebaliknya, deep learning (DL), sebagai sub-bidang dari ML, memiliki kemampuan untuk mempelajari representasi fitur secara otomatis dan hierarkis langsung dari data mentah. Jaringan saraf tiruan mendalam mampu mengidentifikasi pola-pola kompleks dan abstrak (fitur tingkat tinggi) yang mungkin tidak terdeteksi melalui rekayasa fitur manual, menjadikannya sangat efektif dalam mendeteksi anomali dan serangan baru yang tidak memiliki *signature-based* spesifik. Oleh karena itu, sementara ML tradisional membutuhkan intervensi manusia yang lebih besar dalam persiapan data, DL menawarkan solusi yang lebih adaptif dan skalabel untuk menghadapi kompleksitas dan dinamika serangan siber modern yang terus berkembang. Deep learning telah berkembang menjadi pendekatan komputasi paling banyak digunakan dalam bidang machine learning, dan terbukti memberikan hasil yang luar biasa dalam berbagai tugas kognitif kompleks, termasuk penerapannya pada keamanan siber [6].

Penggunaan model hibrida *Convolutional Neural Network* (CNN) dan *Long Short-Term Memory* (LSTM) merupakan strategi yang efektif dalam pengembangan IDS sebab keduanya memiliki kemampuan saling melengkapi untuk mengatasi tantangan deteksi serangan siber modern. Penerapan jaringan hybrid CNN-LSTM dapat meningkatkan akurasi deteksi intrusi jaringan dengan memanfaatkan fitur spasial dan temporal dari lalu lintas data jaringan, yang sulit dicapai oleh metode konvensional [7]. CNN unggul dalam mengekstraksi pola spasial atau lokal yang rumit dari lalu lintas jaringan, misalnya tanda tangan serangan atau karakteristik fitur yang muncul bersamaan dalam satu snapshot data. Sementara itu, LSTM secara efektif mengelola dependensi temporal atau urutan data yang krusial dalam aktivitas jaringan, sehingga model dapat memahami perubahan pola seiring waktu dan mendeteksi anomali yang melibatkan serangkaian kejadian. Arsitektur RNN telah memberikan peningkatan yang signifikan dalam berbagai masalah machine learning yang melibatkan input berurutan (sequential) [8]. Model encoder-decoder berbasis LSTM mampu menangkap konteks temporal dari data sekuensial, yang dibutuhkan untuk tugas pemrosesan bahasa alami maupun analisis pola serangan dalam jaringan [9]. Kombinasi kedua arsitektur ini memungkinkan model untuk menangkap fitur secara hierarkis, dari yang sederhana hingga kompleks, serta menangani dependensi jangka panjang melalui mekanisme gerbang pada LSTM. Oleh karena itu, arsitektur CNN-LSTM sangat sesuai untuk memproses data sekuensial yang kompleks dengan pola lokal dan ketergantungan temporal, menjadikannya solusi menjanjikan untuk identifikasi serangan jaringan yang akurat dan adaptif terhadap evolusi ancaman.

2. METODOLOGI PENELITIAN

Dalam lanskap keamanan siber yang terus berkembang pesat, deteksi serangan jaringan menjadi krusial. Penelitian ini menawarkan pendekatan inovatif untuk meningkatkan akurasi identifikasi ancaman siber, dimulai dengan pemanfaatan dataset komprehensif yang merepresentasikan skenario serangan nyata. Kami kemudian akan menguraikan secara mendalam bagaimana pra-pemrosesan data yang cermat menjadi fondasi utama untuk memastikan kualitas dan keseimbangan data, yang esensial bagi kinerja model. Selanjutnya, inti dari penelitian ini adalah pengembangan model hibrida CNN-LSTM yang dirancang khusus untuk memahami pola spasial dan dependensi temporal dalam lalu lintas jaringan, menjanjikan deteksi serangan yang lebih adaptif. CNN unggul dalam mengenali pola visual spasial dalam data, sementara LSTM berperan dalam analisis data sekuensial, kombinasi ini sangat efektif untuk IDS yang akurat [10]. Terakhir, kami akan menyajikan bagaimana evaluasi model yang terukur dan menyeluruh dilakukan untuk memvalidasi efektivitas pendekatan yang diusulkan.

2.1. Dataset UNSW-NB15

Untuk dataset yang digunakan pada penelitian ini adalah dataset UNSW-NB15. UNSW-NB15 adalah dataset yang dikembangkan untuk mengatasi keterbatasan dari dataset IDS sebelumnya, seperti KDD99 dan NSL-KDD, dalam merepresentasikan ancaman modern pada jaringan. Dataset ini diciptakan di laboratorium Australian Centre for Cyber Security (ACCS) menggunakan IXIA PerfectStorm yang menghasilkan lalu lintas jaringan normal dan serangan sintetik. Dataset ini berisi sembilan kategori serangan (misalnya, *Fuzzers*, *DoS*, dan *Reconnaissance*) dan 49 fitur yang relevan untuk mendeteksi anomali jaringan, sehingga cocok untuk penelitian pada sistem deteksi intrusi modern [11].

2.2. Alat Penelitian

Adapun spesifikasi dari perangkat lunak yang digunakan dalam membangun sistem tersebut adalah sebagai berikut:

System	: Google Colab.
Processor	: Intel(R) Xeon(R) CPU @ 2.00GHz (2 vCPU).
RAM	: 12.7 GB.
GPU	: NVIDIA Tesla T4 (16 GB GDDR6).
Disk	: 112.6 GB.
Maximal Session	: 12 jam.

Namun, ketersediaan GPU T4 tidak selalu dijamin karena sistem berbasis antrian dan *pre-emptible*.

2.3. Pra-pemrosesan Data

Proses pra-pemrosesan data untuk model hybrid CNN-LSTM diinisiasi dengan pengumpulan dan pembersihan data yang bersumber dari file CSV di Google Drive. Data dari berbagai file tersebut kemudian diintegrasikan menjadi satu dataset tunggal. Untuk menjamin kualitasnya, dilakukan eliminasi data duplikat. Analisis data awal dilaksanakan untuk memahami karakteristik dataset,

dengan fokus pada kolom-kolom kategorikal seperti protokol jaringan, layanan, status koneksi, dan kategori serangan, yang memerlukan perlakuan spesifik karena model deep learning hanya dapat memproses input numerik.

Tahap selanjutnya adalah transformasi data kategorikal ke dalam format numerik melalui teknik categorical codes, di mana setiap nilai unik dalam sebuah kolom dipetakan ke kode numerik yang unik. Setelah itu, masalah ketidakseimbangan kelas ditangani menggunakan metode upsampling. Melalui metode ini, data dari kelas minoritas (serangan) direplikasi secara acak hingga jumlahnya setara dengan kelas mayoritas (normal). Pendekatan ini sangat krusial untuk mitigasi bias pada model dan memastikan kemampuan deteksi yang seimbang antara kedua kelas.

Pada langkah final pra-pemrosesan, dataset dibagi menjadi data latih (training) dan data uji (testing) dengan rasio 80:20. Normalisasi fitur kemudian dilakukan menggunakan StandardScaler untuk memastikan seluruh fitur berada pada skala yang seragam. Terakhir, label kelas ditransformasikan ke dalam format one-hot encoding, sehingga data siap digunakan untuk melatih model CNN-LSTM. Seluruh rangkaian proses pra-pemrosesan ini dirancang secara metodis untuk menghasilkan dataset yang bersih, seimbang, dan terstruktur, yang pada akhirnya memaksimalkan efektivitas pembelajaran dari arsitektur hybrid yang digunakan. Parameter-parameter yang digunakan dalam pra-pemrosesan data dirangkum secara detail pada Tabel 1:

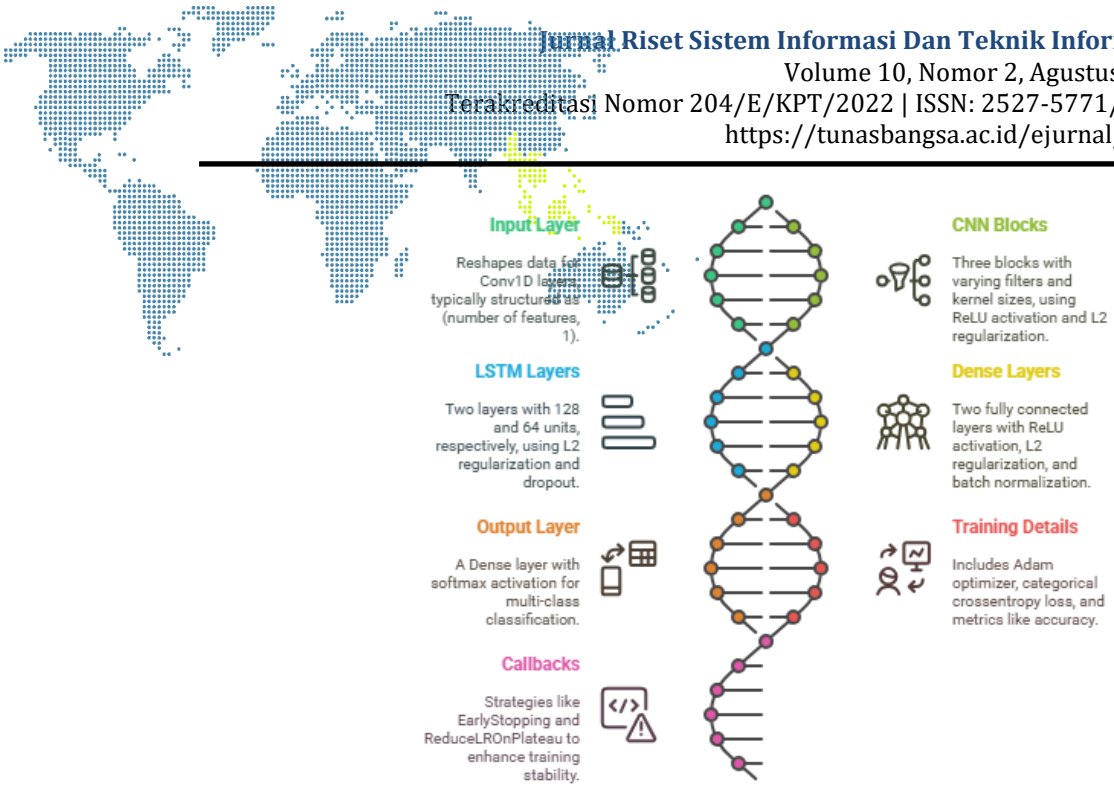
Tabel 1. Parameter Praproses Data

Parameter	Nilai
Train-Test Split	80%-20%
Random State	42
Normalisasi	StandardScaler
Encoding Label	LabelEncoder
Teknik Penyeimbangan Data	Upsampling (Resample)

2.4. Arsitektur Model Hybrid CNN-LSTM

Arsitektur model hibrida ini dirancang secara spesifik untuk mengintegrasikan keunggulan dari Convolutional Neural Networks (CNN) dan Long Short-Term Memory (LSTM) dalam menganalisis data sekuensial yang kompleks, seperti lalu lintas jaringan. Arsitektur dasar CNN yang diusulkan dalam penelitian ini terinspirasi dari implementasi yang tersedia di platform GitHub [12]. Namun, kami merancang ulang konfigurasi lapisan, menambahkan mekanisme regularisasi, serta mengintegrasikannya dengan lapisan LSTM untuk membentuk model hibrida yang lebih robust. Berdasarkan Gambar 1, model ini diawali dengan tiga blok CNN yang disusun secara bertingkat. Setiap blok terdiri dari lapisan Conv1D untuk ekstraksi fitur spasial, seperti pola tanda tangan serangan, yang diikuti oleh BatchNormalization untuk stabilisasi dan akselerasi pelatihan. Selanjutnya, lapisan MaxPooling1D diaplikasikan untuk mereduksi dimensi data dengan tetap mempertahankan fitur-fitur esensial, dan lapisan Dropout dengan laju 0.4 dan 0.5 ditambahkan sebagai teknik regularisasi untuk mitigasi overfitting.

Jurnal Riset Sistem Informasi Dan Teknik Informatika (JURASIK)
Volume 10, Nomor 2, Agustus 2025, pp 528-539
Terakreditasi Nomor 204/E/KPT/2022 | ISSN: 2527-5771/EISSN: 2549-7839
https://tunasbangsa.ac.id/ejurnal/index.php/jurasik



Gambar 1. Arsitektur Model Hybrid CNN-LSTM

Setelah proses ekstraksi fitur spasial oleh CNN, data diproses lebih lanjut oleh dua lapisan LSTM dengan 128 dan 64 unit. Pemanfaatan LSTM menjadi krusial dalam pemodelan dependensi temporal pada data lalu lintas jaringan. Kemampuan LSTM untuk menangani dependensi jangka panjang melalui mekanisme gating memastikan bahwa informasi sekuensial yang signifikan tidak hilang selama pemrosesan , sehingga memungkinkan model untuk mengidentifikasi anomali berdasarkan urutan kejadian dari waktu ke waktu. Fitur-fitur yang telah diekstraksi secara spasial dan temporal kemudian diintegrasikan melalui serangkaian lapisan fully connected (Dense). Lapisan ini juga dilengkapi dengan BatchNormalization dan Dropout untuk meningkatkan robustisitas model. Tahap akhir dari arsitektur ini adalah lapisan output Dense yang menggunakan fungsi aktivasi softmax, sebuah pilihan yang ideal untuk tugas klasifikasi multikelas sebagaimana diimplementasikan dalam penelitian ini.

Untuk proses kompilasi, model ini menggunakan optimizer Adam dengan learning rate 0.0005, yang dipilih karena efisiensinya dalam konvergensi melalui penyesuaian learning rate secara adaptif. Fungsi loss categorical_crossentropy digunakan karena kesesuaiannya dengan problem klasifikasi multikelas. Lebih lanjut, proses pelatihan diperkaya dengan serangkaian callback komprehensif. EarlyStopping dengan patience 15 diterapkan untuk mencegah overfitting dengan memonitor akurasi validasi, sementara ReduceLROnPlateau secara dinamis menyesuaikan learning rate sebagai respons terhadap stagnasi pada validation loss. Selain itu, ModelCheckpoint diimplementasikan untuk menyimpan bobot model dengan performa terbaik berdasarkan akurasi validasi tertinggi. Kombinasi strategis antara arsitektur CNN-LSTM, teknik regularisasi, normalisasi, dan mekanisme callback canggih ini bertujuan untuk menghasilkan sebuah model Intrusion Detection System (IDS) yang tidak hanya akurat dan robust, tetapi juga memiliki kapabilitas generalisasi yang superior dalam mendeteksi beragam jenis

serangan siber. Tabel 2 menyajikan daftar lengkap hyperparameter dan nilai yang diterapkan pada arsitektur model hybrid CNN-LSTM:

Tabel 2. Parameter Arsitektur Model

Layer	Parameter	Nilai
Conv1D (1)	Filters	128
	Kernel Size	3
	Activation	ReLU
	Kernel Regularizer	l2(0.001)
MaxPooling1D (1)	Pool Size	2
Dropout (1)	Rate	0.4
Conv1D (2)	Filters	128
	Kernel Size	2
	Activation	ReLU
	Kernel Regularizer	l2(0.001)
MaxPooling1D (2)	Pool Size	2
Dropout (2)	Rate	0.4
Conv1D (3)	Filters	64
	Kernel Size	1
	Activation	ReLU
	Kernel Regularizer	l2(0.001)
MaxPooling1D (3)	Pool Size	2
LSTM (1)	Units	128
	Return Sequences	TRUE
	Kernel Regularizer	l2(0.001)
Dropout (3)	Rate	0.5
LSTM (2)	Units	64
Dropout (4)	Rate	0.5
Dense (1)	Units	128
	Activation	ReLU
	Kernel Regularizer	l2(0.001)
Dropout (5)	Rate	0.5
Dense (2)	Units	64
	Activation	ReLU
	Kernel Regularizer	l2(0.001)
Dense (Output)	Units	Sesuai jumlah kelas (num_classes)
	Activation	Softmax

2.5. Pelatihan dan Evaluasi Model

Pada tahap pelatihan, model dikonfigurasikan dan dilatih menggunakan fungsi model.fit(). Proses pelatihan ini dijalankan untuk durasi maksimal 30 epoch, yang merepresentasikan iterasi penuh pada keseluruhan dataset pelatihan. Ukuran batch ditetapkan sebesar 64, yang mengindikasikan bahwa pembaruan bobot model dilakukan setelah pemrosesan setiap 64 sampel data. Alokasi data validasi sebesar 20% dari data pelatihan (X_train, y_train) digunakan untuk memonitor performa model terhadap data yang tidak diikutsertakan dalam proses pelatihan utama. Untuk mengoptimalkan proses pelatihan, tiga mekanisme callback diimplementasikan. Early stopping diterapkan untuk mencegah overfitting dengan cara menghentikan pelatihan secara prematur jika kinerja pada set data validasi

tidak menunjukkan perbaikan. Selanjutnya, reduce learning rate (reduce_lr) digunakan untuk menyesuaikan laju pembelajaran secara dinamis apabila validation loss mengalami stagnasi. Terakhir, callback checkpoint berfungsi untuk menyimpan bobot model dengan kinerja terbaik, yang ditentukan berdasarkan pencapaian akurasi validasi tertinggi. Seluruh kemajuan proses pelatihan ditampilkan secara rinci melalui konsol dengan mengaktifkan parameter verbose=1.

Tahap evaluasi merupakan fase krusial untuk mengukur performa dan efektivitas model hibrida CNN-LSTM yang telah dilatih. Langkah pertama dalam evaluasi adalah memuat kembali bobot model terbaik yang sebelumnya telah disimpan selama fase pelatihan (best_enhanced_model.keras). Model tersebut kemudian digunakan untuk menghasilkan prediksi pada data uji (X_test), yang merupakan data yang belum pernah ditemui oleh model. Mengingat arsitektur model dirancang untuk tugas klasifikasi multiclass, luaran prediksi yang berupa probabilitas dikonversi menjadi label kelas diskrit menggunakan fungsi np.argmax baik untuk data prediksi (y_pred) maupun data sebenarnya (y_test).

Kinerja model diukur menggunakan serangkaian metrik evaluasi yang komprehensif, meliputi akurasi, presisi, recall, dan F1-Score. Perhitungan metrik-metrik ini menggunakan pendekatan rata-rata berbobot (weighted average) untuk mengakomodasi sifat multiclass dari dataset. Berikut masing-masing dijelaskan metriks evaluasi yang digunakan [13], [14]:

(a) Akurasi (Accuracy)

Akurasi menyajikan gambaran umum mengenai ketepatan prediksi model secara keseluruhan. Accuracy merupakan metrik dasar yang mengukur tingkat ketepatan prediksi secara keseluruhan, dihitung menggunakan rasio jumlah prediksi benar (true positive dan true negative) terhadap total prediksi yang dapat diformulasikan sebagai:

$$\text{Accuracy} = \frac{\text{TP+TN}}{\text{TP+TN+FP+FN}} \quad (1)$$

(b) Presisi (Precision)

Presisi mengukur rasio prediksi positif yang benar terhadap total prediksi positif yang dibuat oleh model. Precision mengukur ketepatan model dalam memprediksi kelas positif, dengan menghitung proporsi prediksi positif yang benar dari seluruh prediksi positif yang dihasilkan model. Rumus precision dapat dinyatakan sebagai:

$$\text{Precision} = \frac{\text{TP}}{\text{TP+FP}} \quad (2)$$

(c) Perolehan (*Recall*)

Recall mengevaluasi kapasitas model dalam mengidentifikasi seluruh sampel positif yang relevan. Recall atau sensitivity mengukur kemampuan model dalam mengenali seluruh kasus positif yang ada, dihitung sebagai rasio kasus positif yang berhasil diidentifikasi terhadap seluruh kasus positif yang sebenarnya:

Jurnal Riset Sistem Informasi Dan Teknik Informatika (JURASIK)
Volume 10, Nomor 2, Agustus 2025, pp 528-539
Terakreditasi Nomor 204/E/KPT/2022 | ISSN: 2527-5771/EISSN: 2549-7839
https://tunasbangsa.ac.id/ejurnal/index.php/jurasik

$$\text{Recall} = \frac{\text{TP}}{\text{TP+FN}} \quad (3)$$

(d) F1-Score

F1-Score menawarkan nilai tunggal yang menyeimbangkan presisi dan recall, yang sangat relevan untuk dataset dengan distribusi kelas yang tidak seimbang. F1-Score merupakan mean harmonik dari precision dan recall, memberikan nilai tunggal yang menyeimbangkan trade-off antara kedua metrik tersebut. F1-Score sangat berguna ketika diperlukan keseimbangan antara precision dan recall, terutama pada dataset yang tidak seimbang. Rumus F1-Score dapat ditulis sebagai:

$$\text{F1-Score} = 2 \times \frac{\text{Precision} \times \text{Recall}}{\text{Precision+Recall}} \quad (4)$$

Analisis performa juga diperkaya dengan visualisasi data. Confusion matrix yang ditampilkan sebagai heatmap digunakan untuk menganalisis secara mendetail kesalahan klasifikasi yang dilakukan oleh model. Di samping itu, classification report menyajikan rincian nilai presisi, recall, dan F1-Score untuk setiap kelas secara individual. Grafik histori pelatihan yang memplot akurasi dan loss terhadap epoch juga divisualisasikan untuk mengidentifikasi potensi overfitting atau underfitting, serta untuk menilai stabilitas dan konvergensi model selama proses pelatihan. Rincian parameter yang digunakan dapat dilihat pada Tabel 3 dan Tabel 4:

Tabel 3. Parameter Training

Parameter	Nilai
Optimizer	Adam
Learning Rate	0.0005
Loss	'categorical_crossentropy'
Epochs	30
Batch Size	64
Validation Split	20%

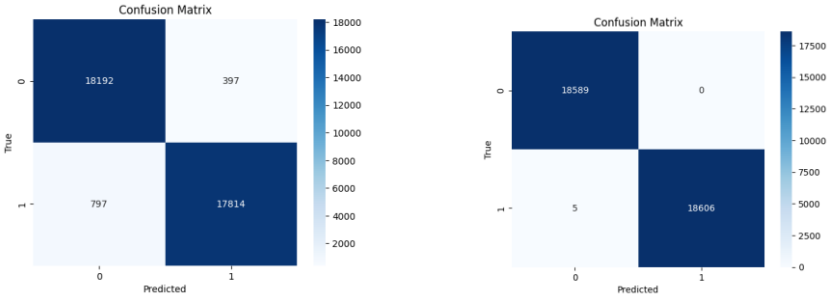
Tabel 4. Parameter Callbacks

Callback	Parameter	Nilai
ModelCheckpoint	Monitor	'val_accuracy'
	Save Best Only	True
	Mode	'max'
	Path	'best_enhanced_model.keras'
EarlyStopping	Monitor	'val_accuracy'
	Patience	15
	Mode	'max'
	Restore Best Weights	True
	Verbose	1
ReduceLROnPlateau	Monitor	'val_loss'
	Factor	0.5
	Patience	5
	Min. learning rate	1e-6
	Verbose	1

Jurnal Riset Sistem Informasi Dan Teknik Informatika (JURASIK)
Volume 10, Nomor 2, Agustus 2025, pp 528-539
Terakreditasi Nomor 204/E/KPT/2022 | ISSN: 2527-5771/EISSN: 2549-7839
https://tunasbangsa.ac.id/ejurnal/index.php/jurasik

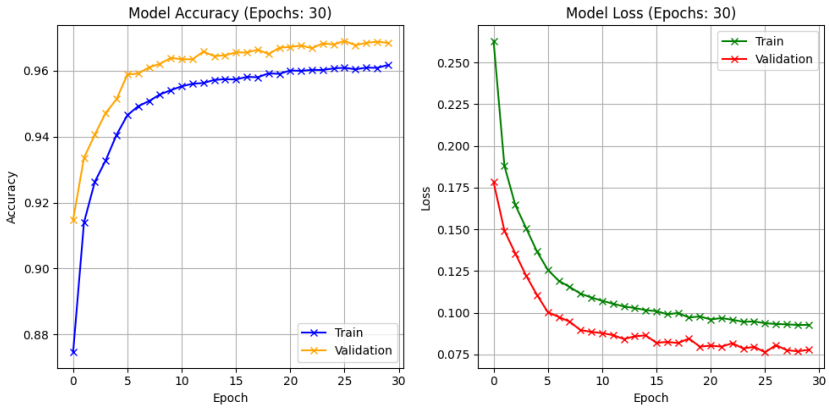
3. HASIL DAN PEMBAHASAN

Evaluasi dilakukan terhadap hasil prediksi pada data uji. Prediksi probabilistik dikonversi menjadi label kelas menggunakan ambang batas 0,5, sementara untuk kasus klasifikasi multi-kelas, dipilih kelas dengan probabilitas tertinggi. Evaluasi performa didasarkan pada metrik akurasi, presisi, recall, dan F1-score.

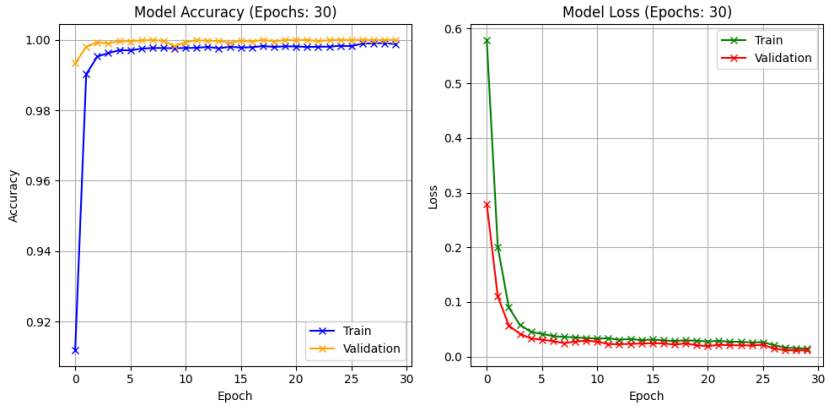


(a) (b)

Gambar 2. Confussion Matrix model : (a) CNN, (b) CNN-LSTM



Gambar 3. Grafik Accuracy dan Loss CNN



Gambar 4. Grafik Accuracy dan Loss CNN-LSTM

Pada Gambar 2, 3 dan 4 dapat disimpulkan bahwa model hybrid CNN-LSTM menunjukkan kinerja yang jauh lebih unggul dibandingkan model CNN standar.

Meskipun model CNN berhasil mencapai tingkat kinerja yang baik, dengan metrik evaluasi seperti Accuracy dan F1-Score berada di sekitar 96%, kurva pembelajarannya menunjukkan bahwa model tersebut belum mencapai konvergensi optimal. Sebaliknya, model CNN-LSTM menunjukkan hasil yang luar biasa dengan metrik Accuracy, Precision, Recall, dan F1-Score yang semuanya mencapai 99%. Keunggulan ini juga sangat jelas terlihat pada grafik pembelajarannya. Kurva akurasi dan loss pada model CNN-LSTM menunjukkan konvergensi yang sangat cepat, di mana nilai akurasi pelatihan dan validasi hampir sempurna berhimpitan mendekati 100%, sementara nilai loss mendekati 0%. Hal ini menandakan bahwa model CNN-LSTM tidak hanya sangat akurat tetapi juga memiliki kemampuan generalisasi yang sangat baik tanpa adanya indikasi overfitting. Penambahan lapisan LSTM memungkinkan model untuk tidak hanya mengekstraksi fitur spasial melalui CNN, tetapi juga memahami dependensi temporal atau urutan data, yang terbukti krusial untuk mencapai tingkat deteksi yang superior. Pada Tabel 5 berisi hasil evaluasi dari lima percobaan yang menunjukkan nilai F1-score di atas 99% secara konsisten:

Tabel 5. Hasil Perbandingan Evaluasi Arsitektur

	CNN	CNN-LSTM
Accuracy	0.9679	0.9999
Precision	0.9681	0.9999
Recall	0.9679	0.9999
F1-Score	0.9679	0.9999

4. SIMPULAN

Berdasarkan hasil penelitian ini, dapat disimpulkan bahwa model hibrida CNN-LSTM menunjukkan kinerja yang jauh lebih unggul secara signifikan dibandingkan dengan model CNN standar untuk identifikasi serangan jaringan pada dataset UNSW-NB15. Dengan pencapaian metrik akurasi, presisi, recall, dan F1-score yang konsisten di atas 99%, model CNN-LSTM terbukti sangat akurat dan memiliki kemampuan generalisasi yang superior tanpa indikasi overfitting, berbeda dengan model CNN yang kinerjanya berada di sekitar 96% dan belum mencapai konvergensi optimal. Keberhasilan ini menegaskan bahwa kombinasi kemampuan CNN dalam mengekstraksi fitur spasial dan LSTM dalam memodelkan dependensi temporal merupakan pendekatan yang sangat efektif untuk deteksi anomali pada data sekuensial yang kompleks seperti lalu lintas jaringan. Untuk penelitian selanjutnya, disarankan agar dilakukan eksplorasi lebih lanjut terhadap arsitektur hibrida ini dengan dataset yang lebih beragam dan skenario serangan yang lebih dinamis, serta mempertimbangkan optimisasi hyperparameter secara lebih ekstensif untuk terus meningkatkan ketahanan dan adaptabilitas model terhadap ancaman siber yang terus berevolusi.

DAFTAR PUSTAKA

[1] S. Indriani Lestariningati, “1. Definisi Keamanan Jaringan,” 2018.
[2] F. S. Mukti, E. Setijadi, A. Affandi, A. Basuki, and M. A. Akbar, “In-Depth Network Traffic Analysis using Machine Learning Perspective: Characterization and

Classification," in *2023 6th International Seminar on Research of Information Technology and Intelligent Systems (ISRITI)*, IEEE, 2023, pp. 415–421.

[3] L. Ashiku and C. Dagli, "Network intrusion detection system using deep learning," *Procedia Comput Sci*, vol. 185, pp. 239–247, 2021.

[4] R. Vinayakumar, M. Alazab, K. P. Soman, P. Poornachandran, A. Al-Nemrat, and S. Venkatraman, "Deep learning approach for intelligent intrusion detection system," *IEEE access*, vol. 7, pp. 41525–41550, 2019.

[5] J. Lansky *et al.*, "Deep learning-based intrusion detection systems: a systematic review," *IEEE Access*, vol. 9, pp. 101574–101599, 2021.

[6] L. Alzubaidi *et al.*, "Review of deep learning: concepts, CNN architectures, challenges, applications, future directions," *J Big Data*, vol. 8, pp. 1–74, 2021.

[7] P. Sun *et al.*, "DL-IDS: Extracting Features Using CNN-LSTM Hybrid Network for Intrusion Detection System," *Security and communication networks*, vol. 2020, no. 1, p. 8890306, 2020.

[8] S. Nosouhian, F. Nosouhian, and A. K. Khoshouei, "A review of recurrent neural network architecture for sequence learning: Comparison between LSTM and GRU," 2021.

[9] D. A. Sulistyo, A. P. Wibawa, D. D. Prasetya, and F. A. Ahda, "LSTM-Based Machine Translation for Madurese-Indonesian," *Journal of Applied Data Sciences*, vol. 4, no. 3, pp. 189–199, 2023.

[10] 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.

[11] N. Moustafa and J. Slay, "UNSW-NB15: a comprehensive data set for network intrusion detection systems (UNSW-NB15 network data set)," in *2015 military communications and information systems conference (MilCIS)*, IEEE, 2015, pp. 1–6.

[12] "AndreiNC05/Intrusion_detection_based_on_artificial-_neural_network_approach: This is the implementation of the thesis for the Computer Science Master from the Technical University of Denmark (DTU)." Accessed: Jan. 21, 2025. [Online]. Available: https://github.com/AndreiNC05/Intrusion_detection_based_on_artificial-_neural_network_approach

[13] "Classification: Accuracy, recall, precision, and related metrics | Machine Learning | Google for Developers." Accessed: Jan. 21, 2025. [Online]. Available: https://developers.google.com/machine-learning/crash-course/classification/accuracy-precision-recall

[14] "Apa Itu Akurasi, Precision, Recall & F1-Score, Rumus & Cara Menghitungnya." Accessed: Jan. 21, 2025. [Online]. Available: https://haloryan.com/blog/apa-itu-akurasi-precision-recall-f1-score-rumus-cara-menghitungnya