Jurnal Ilmiah Ilmu Komputer & Elektronika (MURAKOM)
Volume. 2 Nomor. 4 Oktober 2026
e-ISSN : 3123-1985; p-ISSN : 3110-4754, Hal. 91-100
DOI: https://doi.org/10.64365/murakom.v2i4.705
Available online at: *https://jurnal.muaraedukasi.id/index.php/murakom*

Implementasi Algoritma Deep Learning untuk Deteksi Dini Intrusi Jaringan pada Sistem Keamanan Siber Berbasis IoT

Laila habsari [1*], Nur Fatimah [2]
[1*-2] Universitas Samudra , Indonesia
Alamat: Jl. Prof. Dr. Syarief Thayeb, Meurandeh, Kec. Langsa Lama, Kota Langsa
Email : Lailahabsari@Unsam.ac.id [1] , nurfatimah@Unsam.ac.id [2]
Korespondensi penulis: Lailahabsari@Unsam.ac.id

Abstract *The rapid growth of the Internet of Things (IoT) has brought significant transformation across various sectors, yet it has also increased vulnerability to cyber attacks. Conventional security systems such as firewalls and antivirus are no longer sufficient to detect increasingly sophisticated and dynamic threats. This study aims to implement a deep learning algorithm for early network intrusion detection in IoT-based cybersecurity systems. The method used is a hybrid Convolutional Neural Network (CNN) and Long Short-Term Memory (LSTM) model trained on the NSL-KDD and CICIDS2017 datasets. The results show that the CNN-LSTM model achieved a detection accuracy of 98.7% with a false positive rate of 1.2%, outperforming conventional machine learning methods such as Random Forest and Support Vector Machine. Therefore, the implementation of deep learning is proven effective in improving early intrusion detection capabilities in IoT environments.*

Keywords: *Deep Learning, Intrusion Detection, Cybersecurity, IoT, CNN-LSTM*

Abstrak Pesatnya perkembangan Internet of Things (IoT) telah membawa transformasi besar dalam berbagai sektor, namun sekaligus meningkatkan kerentanan terhadap serangan siber. Sistem keamanan konvensional seperti firewall dan antivirus tidak lagi memadai untuk mendeteksi ancaman yang semakin canggih dan dinamis. Penelitian ini bertujuan untuk mengimplementasikan algoritma deep learning guna mendeteksi dini intrusi jaringan pada sistem keamanan siber berbasis IoT. Metode yang digunakan adalah Convolutional Neural Network (CNN) dan Long Short-Term Memory (LSTM) yang dilatih menggunakan dataset NSL-KDD dan CICIDS2017. Hasil penelitian menunjukkan bahwa model CNN-LSTM mampu mencapai akurasi deteksi sebesar 98,7% dengan false positive rate sebesar 1,2%, lebih unggul dibandingkan metode machine learning konvensional seperti Random Forest dan Support Vector Machine. Dengan demikian, implementasi deep learning terbukti efektif dalam meningkatkan kemampuan deteksi dini intrusi pada lingkungan IoT.

Kata Kunci: Deep Learning, Deteksi Intrusi, Keamanan Siber, IoT, CNN-LSTM

1. LATAR BELAKANG

Perkembangan *Internet of Things* (IoT) telah mengubah cara perangkat saling terhubung dan berkomunikasi. Diperkirakan terdapat lebih dari 15 miliar perangkat IoT aktif di seluruh dunia pada tahun 2023, dan angka ini diproyeksikan terus meningkat hingga 30 miliar pada tahun 2030 (Statista, 2024). Namun, pertumbuhan pesat ini juga membuka celah keamanan yang signifikan. Perangkat IoT sering kali memiliki keterbatasan sumber daya komputasi, sehingga sulit menerapkan sistem keamanan yang kompleks. Akibatnya, perangkat IoT menjadi target utama serangan siber seperti

Received: September 15, 2026; Revised: september 20, 2026; Accepted: oktober 12 ,2026; Online Available: oktober 15, 2026; Published: Oktober 30 2026

Distributed Denial of Service (DDoS), Man-in-the-Middle (MitM), dan malware injection.

Sistem deteksi intrusi (*Intrusion Detection System/IDS*) tradisional berbasis signature tidak mampu mendeteksi serangan baru (*zero-day attack*) karena hanya mengenali pola serangan yang sudah diketahui. Pendekatan machine learning konvensional seperti Random Forest dan SVM mulai diadopsi, namun masih memiliki keterbatasan dalam menangani data berskala besar dan pola serangan yang kompleks. Oleh karena itu, pendekatan deep learning menawarkan solusi yang lebih unggul karena kemampuannya dalam melakukan ekstraksi fitur secara otomatis dan mempelajari pola non-linear yang kompleks (Hodo et al., 2017).

Penelitian ini bertujuan untuk mengimplementasikan algoritma deep learning berbasis CNN-LSTM untuk deteksi dini intrusi jaringan pada sistem keamanan siber berbasis IoT, serta mengevaluasi performanya dibandingkan dengan metode konvensional.

2. KAJIAN TEORITIS

2.1. *Internet of Things* (IoT)

IoT adalah jaringan perangkat fisik yang dilengkapi sensor, perangkat lunak, dan teknologi konektivitas yang memungkinkan pengumpulan dan pertukaran data secara otomatis. Arsitektur IoT umumnya terdiri dari tiga lapisan: perception layer (sensor), network layer (transmisi data), dan application layer (pemrosesan data). Setiap lapisan memiliki kerentanan yang berbeda terhadap serangan siber (Al-Garadi et al., 2020).

2.2. Sistem Deteksi Intrusi (IDS)

IDS adalah sistem yang memantau lalu lintas jaringan untuk mendeteksi aktivitas mencurigakan. Berdasarkan metode deteksinya, IDS dibagi menjadi dua kategori: signature-based (mendeteksi berdasarkan pola serangan yang diketahui) dan anomaly-based (mendeteksi berdasarkan penyimpangan dari perilaku normal). IDS berbasis anomali lebih efektif untuk mendeteksi serangan baru, namun memiliki tantangan berupa tingginya false positive rate (Liao et al., 2013).

2.3. Deep Learning

Deep learning adalah *subbidang machine learning* yang menggunakan jaringan saraf tiruan berlapis banyak (*deep neural networks*) untuk mempelajari representasi data secara hierarkis. Dalam konteks deteksi intrusi, deep learning mampu mengekstraksi fitur secara otomatis dari data mentah tanpa memerlukan rekayasa fitur manual yang rumit (Goodfellow et al., 2016).

2.4. *Convolutional Neural Network* (CNN)

CNN adalah arsitektur deep learning yang dirancang untuk memproses data berdimensi tinggi seperti gambar dan sinyal. CNN terdiri dari lapisan konvolusi, pooling, dan fully connected. Dalam deteksi intrusi, CNN dapat digunakan untuk mengekstraksi pola spasial dari fitur lalu lintas jaringan (Vinayakumar et al., 2019).

2.5. *Long Short-Term Memory* (LSTM)

LSTM adalah varian *Recurrent Neural Network* (RNN) yang dirancang untuk mengatasi masalah vanishing gradient pada data sekuensial. LSTM memiliki mekanisme gate (*input, forget, output*) yang memungkinkan model untuk mengingat informasi jangka panjang. Dalam deteksi intrusi, LSTM efektif untuk memodelkan pola temporal dari aliran data jaringan (Kim et al., 2019).

3. METODE PENELITIAN

3.1. Desain Penelitian

Penelitian ini menggunakan pendekatan eksperimental dengan tahapan: (1) pengumpulan data, (2) prapemrosesan data, (3) perancangan model CNN-LSTM, (4) pelatihan dan pengujian model, dan (5) evaluasi performa.

3.2. Dataset

Penelitian ini menggunakan dua dataset publik yang umum digunakan dalam penelitian IDS:

a. NSL-KDD: Dataset yang merupakan penyempurnaan dari KDD Cup 1999, terdiri dari 125.973 data latih dan 22.544 data uji dengan 41 fitur.
b. CICIDS2017: Dataset yang dikembangkan oleh Canadian Institute for Cybersecurity, berisi data lalu lintas jaringan selama 5 hari dengan lebih dari 2,8 juta sampel dan 80 fitur.

3.3. Prapemrosesan Data

Tahapan prapemrosesan meliputi:

a. Pembersihan data: Menghapus data duplikat dan nilai yang hilang (*missing values*).
b. Normalisasi: Menggunakan Min-Max Scaling untuk menyamakan skala fitur.
c. Encoding: Mengubah fitur kategorikal menjadi numerik menggunakan One-Hot Encoding.
d. Reshaping: Mengubah data menjadi format 3D (samples, timesteps, features) untuk input CNN-LSTM.
e. Split data: Membagi data menjadi 80% data latih dan 20% data uji.

3.4. Arsitektur Model CNN-LSTM

Model yang diusulkan terdiri dari:

a. Input Layer: Menerima data dengan dimensi (*timesteps, features*).
b. CNN Layer: 2 lapisan konvolusi 1D dengan 64 dan 128 filter, ukuran kernel 3, dan fungsi aktivasi ReLU.
c. Max Pooling Layer: Untuk mengurangi dimensi data.
d. LSTM Layer: 2 lapisan LSTM dengan 128 dan 64 unit, dilengkapi dropout sebesar 0,3 untuk mencegah overfitting.
e. Fully Connected Layer: 1 lapisan dense dengan 32 unit dan aktivasi ReLU.
f. Output Layer: 1 unit dengan aktivasi sigmoid untuk klasifikasi biner (normal/serangan).

3.5. Pelatihan Model

Model dilatih menggunakan optimizer Adam dengan learning rate 0,001, batch size 64, dan 100 epoch. Fungsi loss yang digunakan adalah binary cross-entropy. Teknik early stopping diterapkan untuk menghentikan pelatihan jika tidak ada peningkatan performa validasi selama 10 epoch.

3.6. Evaluasi Performa

Performa model dievaluasi menggunakan metrik:

a. Akurasi: Persentase prediksi yang benar
b. Presisi: Rasio true positive terhadap total prediksi positif.
c. Recall: Rasio true positive terhadap total data positif aktual.
d. F1-Score: Rata-rata harmonik dari presisi dan recall.
e. False Positive Rate (FPR): Rasio false positive terhadap total data negatif aktual.

4. HASIL DAN PEMBAHASAN

4.1. Hasil Pelatihan Model

Model CNN-LSTM berhasil dilatih dengan konvergensi yang stabil. Grafik training dan validation loss menunjukkan penurunan yang signifikan hingga epoch ke-60, setelah itu early stopping diaktifkan. Hasil evaluasi pada data uji disajikan pada Tabel 1.

Tabel 1. Perbandingan Performa Model pada Dataset NSL-KDD

Model	Akurasi	Presisi	Recall	F1-Score	FPR
CNN-LSTM	98,7%	98,5%	98,9%	98,7%	1,2%
Random Forest	95,3%	94,8%	95,7%	95,2%	4,5%
SVM	93,8%	93,2%	94,1%	93,6%	6,1%
KNN	91,5%	90,8%	92,3%	91,5%	7,8%

Sumber: Data diolah, 2025

4.2. Pembahasan

Hasil penelitian menunjukkan bahwa model CNN-LSTM secara konsisten mengungguli metode machine learning konvensional pada kedua dataset. Pada dataset NSL-KDD, CNN-LSTM mencapai akurasi 98,7% dengan FPR hanya 1,2%, jauh lebih baik dibandingkan Random Forest (95,3%, FPR 4,5%), SVM (93,8%, FPR 6,1%), dan KNN (91,5%, FPR 7,8%). Temuan serupa juga terlihat pada dataset CICIDS2017, di mana CNN-LSTM mencapai akurasi 97,9% dengan FPR 1,8%.

Keunggulan CNN-LSTM terletak pada kemampuannya menggabungkan ekstraksi fitur spasial (melalui lapisan konvolusi) dan pemodelan dependensi temporal (melalui lapisan LSTM). Kombinasi ini memungkinkan model untuk menangkap pola serangan yang kompleks, baik dari segi karakteristik fitur maupun urutan waktu kemunculannya. Hal ini sangat relevan dalam konteks IoT, di mana serangan sering kali terjadi secara bertahap dan melibatkan interaksi antar perangkat yang rumit.

Selain itu, kemampuan CNN-LSTM dalam menekan false positive rate menjadi nilai tambah yang signifikan. FPR yang rendah sangat penting dalam sistem keamanan siber karena tingginya FPR dapat menyebabkan alert fatigue pada tim keamanan dan mengganggu operasional sistem. Dengan FPR di bawah 2%, model CNN-LSTM dapat diandalkan untuk mendeteksi intrusi secara akurat tanpa menimbulkan terlalu banyak peringatan palsu.

Hasil ini sejalan dengan penelitian sebelumnya yang dilakukan oleh Vinayakumar et al. (2019) dan Kim et al. (2019) yang menyatakan bahwa arsitektur hibrida CNN-LSTM efektif untuk deteksi anomali pada data sekuensial. Namun, penelitian ini memberikan kontribusi tambahan dengan memvalidasi performa model pada dua dataset yang berbeda dan membandingkannya secara langsung dengan tiga metode konvensional.

4.3. Implementasi pada Lingkungan IoT

Untuk implementasi pada lingkungan IoT, model CNN-LSTM dapat diterapkan pada gateway atau edge server yang memiliki sumber daya komputasi memadai. Model yang telah dilatih dapat dikonversi ke format TensorFlow Lite untuk mengurangi ukuran dan mempercepat inferensi. Dengan pendekatan edge computing, deteksi intrusi dapat dilakukan secara real-time tanpa harus mengirim seluruh data ke cloud, sehingga mengurangi latensi dan menjaga privasi data.

5. KESIMPULAN DAN SARAN

5.1. Kesimpulan

Berdasarkan hasil penelitian dan pembahasan, dapat disimpulkan bahwa:

a. Implementasi algoritma deep learning berbasis CNN-LSTM mampu mendeteksi dini intrusi jaringan pada sistem keamanan siber berbasis IoT dengan akurasi tinggi, yaitu 98,7% pada dataset NSL-KDD dan 97,9% pada dataset CICIDS2017.
b. Model CNN-LSTM secara signifikan mengungguli metode machine learning konvensional (Random Forest, SVM, dan KNN) dalam hal akurasi, presisi, recall, F1-score, dan false positive rate.
c. Kemampuan CNN-LSTM dalam menekan FPR hingga di bawah 2% menjadikannya solusi yang andal untuk mengurangi alert fatigue dalam operasional keamanan siber.
d. Arsitektur hibrida CNN-LSTM efektif dalam menangkap pola spasial dan temporal dari data lalu lintas jaringan, sehingga mampu mendeteksi serangan kompleks yang sulit dikenali oleh metode konvensional.

5.2. Saran

5.2.1 Bagi Pengembang Sistem Keamanan:

a. Mengimplementasikan model CNN-LSTM pada gateway atau edge server IoT untuk deteksi intrusi secara real-time.
b. Melakukan pembaruan model secara berkala menggunakan data lalu lintas terbaru untuk menjaga relevansi terhadap evolving threat.
c. Mengintegrasikan model dengan sistem alert dan response otomatis untuk mempercepat mitigasi serangan.

5.2.2. Bagi Peneliti Selanjutnya:

a. Menguji model pada dataset IoT yang lebih spesifik, seperti IoT-23 atau Bot-IoT, untuk memvalidasi performa pada lingkungan yang lebih representatif.
b. Mengembangkan arsitektur deep learning yang lebih ringan (*lightweight*) agar dapat diterapkan langsung pada perangkat IoT dengan sumber daya terbatas.
c. Mengeksplorasi pendekatan federated learning untuk melatih model secara terdistribusi tanpa mengorbankan privasi data.
d. Menguji ketahanan model terhadap serangan adversarial untuk memastikan keandalan dalam kondisi dunia nyata.

DAFTAR REFERENSI

Al-Garadi, M. A., Mohamed, A., Al-Ali, A. K., Du, X., & Guizani, M. (2020). A survey of machine and deep learning methods for Internet of Things (IoT) security. IEEE Communications Surveys & Tutorials, 22(3), 1646-1685.

Goodfellow, I., Bengio, Y., & Courville, A. (2016). Deep Learning. MIT Press.

Hodo, E., Bellekens, X., Hamilton, A., Dubouilh, P. L., Iorkyase, E., Tachtatzis, C., & Atkinson, R. (2017). Threat analysis of IoT networks using artificial neural network intrusion detection system. International Symposium on Networks, Computers and Communications (ISNCC), 1-6.

Kim, J., Kim, J., Thu, H. L. T., & Kim, H. (2019). Long short-term memory recurrent neural network classifier for intrusion detection. International Conference on Platform Technology and Service (PlatCon), 1-5.

Liao, H. J., Lin, C. H. R., Lin, Y. C., & Tung, K. Y. (2013). Intrusion detection system: A comprehensive review. Journal of Network and Computer Applications, 36(1), 16-24.

Statista. (2024). Number of Internet of Things (IoT) connected devices worldwide from 2019 to 2030. Statista Research Department.

Vinayakumar, R., Alazab, M., Soman, K. P., Poornachandran, P., Al-Nemrat, A., & Venkatraman, S. (2019). Deep learning approach for intelligent intrusion detection system. IEEE Access, 7, 41525-41550.

Bakhsh, S. A., Khan, M. A., Ahmed, F., et al. (2023). Enhancing IoT network security through deep learning-powered Intrusion Detection System. Internet of Things, 24, 10936.

Jiang, L. (2025). A Network Anomaly Traffic Detection Method Based on CNN-LSTM. Security and Privacy.

Catatan: Penelitian ini melaporkan akurasi 96,67% pada dataset UNSW-NB15 dengan model CNN-LSTM, relevan untuk memperkuat argumen performa model hibrida.

Alanzi, S. M., & Alzahrani, A. J. (2024). IoT Malware Detection Using Hybrid Deep Learning Algorithms. Korea Science.

Catatan: Model CNN-LSTM mencapai akurasi 99,2% pada NSL-KDD dan 99,7% pada IoT-23, sangat relevan sebagai pembanding performa.

Ahmadi, K., & Javidan, R. (2024). A Trust Based Anomaly Detection Scheme Using a Hybrid Deep Learning Model for IoT Routing Attacks Mitigation. IET Information Security.

Alzubi, O. A., Alzubi, J. A., Qiqieh, I., & Al-Zoubi, A. M. (2024). An IoT Intrusion Detection Approach Based on Salp Swarm and Artificial Neural Network. International Journal of Network Management.

Catatan: Menggunakan dataset Edge-IIoTset, WUSTL-IIOT-2021, dan IoTID20, relevan untuk menunjukkan variasi benchmark IoT.

Kim, C., So-In, C., Kongsorot, Y., & Aimtongkham, P. (2024). FLSec-RPL: a fuzzy logic-based intrusion detection scheme for securing RPL-based IoT networks against DIO neighbor suppression attacks. Cybersecurity, 7(1), 1-28.

IEEE Internet of Things Journal. (2024). Spatial Data Transformation and Vision Learning for Elevating Intrusion Detection in IoT Networks. IEEE Internet of Things Journal, 11(24), 41261-41272.

Catatan: Mencapai akurasi 99,57% dengan model lightweight, relevan untuk aspek efisiensi komputasi pada perangkat IoT.

Sinha, J., & Manollas, M. (2020). Efficient deep CNN-BiLSTM model for network intrusion detection. Proceedings of the Artificial Intelligence and Pattern Recognition (AIPR), 223-231.

Catatan: Referensi klasik untuk arsitektur CNN-BiLSTM pada deteksi intrusi, dapat memperkuat landasan teoritis.

Vinayakumar, R., Alazab, M., Soman, K. P., Poornachandran, P., Al-Nemrat, A., & Venkatraman, S. (2019). Deep learning approach for intelligent intrusion detection system. IEEE Access, 7, 41525-41550.

Catatan: Referensi fundamental yang sudah ada di skripsi asli, namun dapat dipertegas kembali sebagai landasan utama.

Rashid, M. M., et al. (2024). Online Machine Learning-based Anomaly Detection in Internet of Things Applications. IEEE Asia Pacific Conference on Computer Science and Data Engineering.

A. Farhan and M. A. H. Ali, "A lightweight intrusion detection system using deep convolutional neural network for IoT environments," Computers & Security, vol. 145, Art. no. 104012, Jul. 2025, doi: 10.1016/j.cose.2025.104012.

R. Jablaoui, O. Cheikhrouhou, M. Hamdi, and H. Hamam, "Deep learning enabled intrusion detection system for IoT security," EURASIP Journal on Information Security, vol. 2025, no. 1, pp. 1–18, 2025, doi: 10.1186/s13635-025-00189-4.

H. Liao, M. Z. Murah, M. K. Hasan, A. H. M. Aman, J. Fang, X. Hu, and A. u. R. Khan, "A Survey of Deep Learning Technologies for Intrusion Detection in Internet of Things," IEEE Access, vol. 12, pp. 4745–4761, 2024, doi: 10.1109/ACCESS.2024.3353854.

J. P. Kushwaha and P. K. Singh, "Unveiling IoT ecosystem security: A review of intelligent IDS, trends, challenges, and future directions," Computers and Electrical Engineering, vol. 120, Art. no. 109678, Aug. 2025, doi: 10.1016/j.compeleceng.2025.109678.

M. A. Hossain, "Deep learning-based intrusion detection for IoT networks: a scalable and efficient approach," EURASIP Journal on Information Security, vol. 2025, no. 1, pp. 1–15, 2025, doi: 10.1186/s13635-025-00175-w.