MIND (Multimedia Artificial Intelligent Networking Database) Journal

MIND Journal | ISSN (p): 2528-0015 | ISSN (e): 2528-0902 | Vol. 11 | No. 1 | Halaman 77 - 87
DOI :https://doi.org/10.26760/mindjournal.v11i1.77-87 Juni 2026

Deteksi Botnet pada Internet of Things Menggunakan Algoritma Long Short-Term Memory

VINSENSIUS YOGA DANAR WIJAYA, GOENAWAN BROTOSAPUTRO

Fakultas Teknologi Informasi, Universitas Budi Luhur Jakarta, Indonesia
Email: 2011600729@student.budiluhur.ac.id

Received 16 Maret 2026 **|** *Revised* 26 May 2026 **|** *Accepted* 4 June 2026

ABSTRAK

Pertumbuhan Internet of Things (IoT) meningkatkan konektivitas perangkat sekaligus memperluas risiko serangan botnet. Keterbatasan sumber daya pada perangkat IoT menyebabkan metode deteksi tradisional kurang efektif dalam mengenali pola serangan yang dinamis. Penelitian ini mengusulkan model deteksi botnet berbasis Long Short-Term Memory (LSTM) dengan memanfaatkan karakteristik temporal trafik jaringan. Dataset yang digunakan merupakan subset Bot-IoT sebanyak 14.000 data yang terdiri atas trafik normal dan serangan botnet. Tahap pengolahan data meliputi pembersihan data, seleksi fitur, normalisasi Min-Max, dan pembentukan sequence. Hasil pengujian menunjukkan bahwa model LSTM mencapai akurasi 95,89% dan nilai AUC 0,97. Temuan ini menunjukkan bahwa LSTM efektif untuk mendeteksi aktivitas botnet pada lingkungan IoT dengan keterbatasan sumber daya komputasi.

***Kata kunci**: Internet of Things, Botnet Detection, Deep Learning, Long Short-Term Memory, Intrusion Detection System*

ABSTRACT

The rapid growth of the Internet of Things (IoT) has increased device connectivity while expanding the risk of botnet attacks. Limited computational resources in IoT devices reduce the effectiveness of traditional detection methods in identifying dynamic attack patterns. This study proposes a Long Short-Term Memory (LSTM)-based botnet detection model by leveraging the temporal characteristics of network traffic. A subset of the Bot-IoT dataset consisting of 14,000 normal and botnet traffic records was used. Data preprocessing included cleaning, feature selection, Min-Max normalization, and sequence construction. Experimental results show that the proposed LSTM model achieved an accuracy of 95.89% and an AUC of 0.97. These findings indicate that LSTM is effective for detecting botnet activities in IoT environments with limited computational resources.

***Keywords**: Internet of Things, Botnet Detection, Deep Learning, Long Short-Term Memory, Intrusion Detection System*

1. PENDAHULUAN

Kemajuan dalam *Internet of Things* (IoT) memungkinkan beragam perangkat terhubung dan saling bertukar informasi secara langsung, sehingga meningkatkan efisiensi di berbagai sektor seperti industri, kesehatan, dan rumah pintar(**Hadiningrum et al., 2025**; **Wazzan et al., 2021**). Namun, peningkatan konektivitas ini juga diikuti oleh meningkatnya risiko keamanan siber, khususnya serangan botnet. *Botnet* merupakan jaringan perangkat yang telah terinfeksi dan dikendalikan oleh penyerang untuk melakukan aktivitas berbahaya seperti *distributed denial-of-service* (DDoS), pencurian data, dan penyebaran *malware*.

Sebagian besar perangkat IoT memiliki batasan pada sumber daya seperti kapasitas penyimpanan dan kemampuan pemrosesan yang terbatas **(Wazzan et al., 2021**). Kondisi ini menyebabkan metode deteksi berbasis *signature* dan *rule-based* (misalnya *intrusion detection system* konvensional) kurang efektif dalam mendeteksi pola serangan yang dinamis dan berbasis perilaku. Oleh karena itu, pendekatan berbasis *machine learning* dan *deep learning* mulai banyak digunakan untuk meningkatkan kemampuan deteksi.

Berbagai penelitian sebelumnya telah menggunakan teknik deep learning seperti *Convolutional Neural Network* (CNN), *Recurrent Neural Network* (RNN), dan gabungan CNN-LSTM untuk menangkap serangan botnet di jaringan IoT (**Alkahtani & Aldhyani, 2021**). Model-model tersebut menunjukkan performa yang tinggi dalam klasifikasi trafik jaringan. Namun, model *hybrid* seperti CNN-LSTM memiliki kompleksitas komputasi yang lebih besar sehingga kurang optimal untuk diterapkan pada perangkat IoT yang memiliki keterbatasan sumber daya.

Sebaliknya, *Long Short-Term Memory* (LSTM) yang merupakan elemen dari *Recurrent Neural Network* dibuat untuk menangkap hubungan temporal dalam data berurutan (**Hasas et al., 2024**). Karakteristik ini menjadikan LSTM cocok digunakan dalam analisis trafik jaringan yang memiliki pola berbasis waktu. Selain itu, arsitektur LSTM relatif lebih sederhana dibandingkan model *hybrid* sehingga lebih sesuai untuk implementasi pada lingkungan IoT. Selain mampu menangkap dependensi temporal pada data sekuensial, arsitektur *Long Short-Term Memory* (LSTM) dipilih karena memiliki kompleksitas komputasi yang lebih rendah dibandingkan model *hybrid* seperti CNN-LSTM. Pada arsitektur CNN-LSTM, *convolution layer* digunakan untuk melakukan ekstraksi fitur sebelum proses pembelajaran temporal sehingga membutuhkan parameter dan proses komputasi yang lebih besar.

Sementara itu, model LSTM pada penelitian ini hanya menggunakan dua *hidden layer* tanpa convolution layer tambahan sehingga arsitekturnya menjadi lebih sederhana. Kesederhanaan arsitektur tersebut menjadi penting pada lingkungan Internet of Things (IoT) yang memiliki keterbatasan sumber daya seperti CPU, memori, dan konsumsi daya. Untuk mendukung efisiensi komputasi tersebut, penelitian ini menggunakan konfigurasi model yang terdiri dari dua hidden layer LSTM dengan ukuran 64 dan 32 unit, timestep 10, *batch size* 32, dan *optimizer Adam*. Konfigurasi tersebut dirancang untuk menghasilkan performa klasifikasi yang baik tanpa meningkatkan kompleksitas model secara berlebihan.

Penelitian ini tidak melakukan implementasi langsung terhadap model CNN-LSTM sebagai pembanding komputasional. Namun berdasarkan karakteristik arsitektur pada penelitian sebelumnya, CNN-LSTM memiliki kompleksitas parameter yang lebih tinggi dibandingkan LSTM tunggal. Oleh karena itu, penelitian ini memfokuskan penggunaan LSTM untuk memperoleh keseimbangan antara performa deteksi dan efisiensi komputasi pada lingkungan IoT.
Untuk memperjelas posisi penelitian ini, Tabel 1 menunjukkan perbandingan beberapa penelitian terkait.

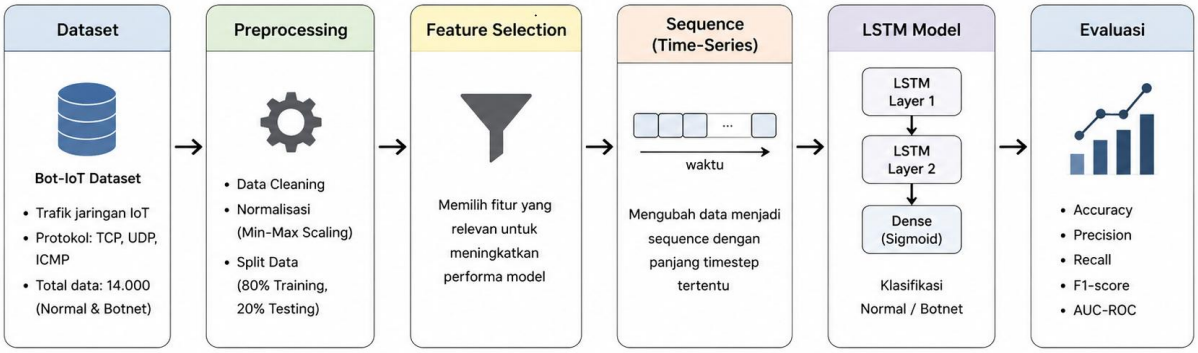
Tabel 1. Perbandingan Penelitian

Penelitian	Metode	Dataset	Accuracy
Alkahtani & Aldhyani (2021)	CNN-LSTM	IoT Botnet	94%
Hasas et al. (2024)	LSTM + RF	Network IDS	95%
Hussain et al. (2025)	CNN-LSTM	IoT Network	95.5%
Penelitian ini	LSTM	Bot-IoT	95.89%

Berdasarkan Tabel 1, model CNN-LSTM menunjukkan performa yang tinggi namun memiliki kompleksitas komputasi yang lebih besar. Sementara itu, pendekatan LSTM dalam penelitian ini mampu memberikan performa yang kompetitif dengan arsitektur yang lebih sederhana, sehingga lebih sesuai untuk implementasi pada perangkat IoT yang memiliki keterbatasan sumber daya. Berdasarkan latar belakang tersebut, penelitian ini bertujuan untuk mengimplementasikan model LSTM dalam mendeteksi aktivitas botnet pada jaringan IoT serta mengevaluasi performanya menggunakan metrik seperti *accuracy, precision, recall, F1-score,* dan AUC.

2. METODOLOGI PENELITIAN

Penelitian ini menerapkan metode eksperimen kuantitatif untuk merancang sistem deteksi botnet dengan menggunakan *deep learning* di dalam ekosistem *Internet of Things* (IoT). Prosedur penelitian dilaksanakan melalui beberapa langkah kunci yang meliputi pengumpulan data, *preprocessing*, pemodelan, dan penilaian model.



Gambar 1. Alur Penelitian

Berdasarkan Gambar 1, penelitian dimulai dari tahap pengumpulan dataset Bot-IoT, dilanjutkan dengan *preprocessing data*, pembentukan *sequence*, pelatihan model LSTM, dan evaluasi performa model. Dataset yang digunakan adalah Bot-IoT yang tersedia pada platform Kaggle dan dihasilkan dari simulasi lingkungan IoT yang mencakup berbagai perangkat seperti sensor, kamera, dan *node* jaringan virtual. Dataset ini berisi trafik jaringan berbasis protokol TCP, UDP, dan ICMP yang merepresentasikan komunikasi antar perangkat IoT. Dataset ini mencakup aktivitas normal serta berbagai jenis serangan botnet seperti reconnaissance dan denial-of-service yang memiliki pola temporal tertentu dalam trafik jaringan.

Dataset Bot-IoT dikembangkan melalui simulasi lingkungan *Internet of Things* (IoT) yang terdiri dari berbagai perangkat *virtual* seperti sensor, kamera CCTV, *smart home devices*, dan node jaringan yang saling terhubung melalui protokol TCP/IP. Dataset ini merepresentasikan komunikasi jaringan normal maupun aktivitas serangan *botnet* pada lingkungan IoT. Jenis

serangan dalam dataset meliputi *Distributed Denial of Service* (DDoS), DoS, *reconnaissance*, dan *information theft*. Serangan tersebut menghasilkan pola trafik temporal seperti peningkatan packet rate, lonjakan jumlah *byte* transmisi, serta komunikasi berulang dalam interval waktu tertentu. Penelitian ini menggunakan subset sebanyak 14.000 data yang terdiri dari 7.000 trafik normal dan 7.000 trafik *botnet*. Distribusi data diseimbangkan untuk menghindari bias klasifikasi sehingga model dapat mempelajari kedua kelas secara proporsional.

Tabel 2. Deskripsi Fitur Dataset

No	Fitur	Deskripsi
1	pkts	Jumlah total paket
2	bytes	Total byte transmisi
3	dur	Durasi komunikasi
4	rate	Laju transfer data
5	srate	Laju paket sumber
6	drate	Laju paket tujuan
7	spkts	Paket dari sumber
8	dpkts	Paket dari tujuan
9	sbytes	Byte dari sumber
10	dbytes	Byte dari tujuan
11	pkt_ratio	Rasio paket sumber/tujuan
12	byte_ratio	Rasio byte sumber/tujuan
13	bytes_per_pkt	Rata-rata byte per paket

Fitur-fitur tersebut merepresentasikan karakteristik statistik dan perilaku komunikasi jaringan yang relevan untuk membedakan antara trafik normal dan serangan *botnet.*

Tabel 3. Distribusi Dataset Penelitian

Kategori	Jumlah
Normal	7000
Botnet	7000
Total	14000

Data kemudian diproses melalui tahap pembersihan, seleksi fitur, serta normalisasi Min-Max untuk memastikan konsistensi nilai fitur. Normalisasi dilakukan menggunakan Persamaan (1)

$$x' = \frac{x - x_{min}}{x_{max} - x_{min}} \quad (1)$$

Dataset dibagi menjadi data latih dan uji (80:20), kemudian dibentuk menjadi *sequence* dengan panjang *timestep* 10. Model LSTM terdiri dari dua *layer* (64 dan 32 unit) dan *layer Dense* dengan aktivasi sigmoid. Model dilatih dengan memanfaatkan *optimizer Adam* bersama dengan fungsi *loss binary cross-entropy*.

Tabel 4. Konfigurasi Model LSTM

Parameter	Nilai
Epoch	20
Batch Size	32
Optimizer	Adam
Learning Rate	0.001
Timestep	10
Hidden Layer	64 dan 32 unit
Fungsi Aktivasi Output	Sigmoid
Loss Function	*Binary Cross-Entropy*

Konfigurasi model tersebut dirancang untuk menghasilkan performa klasifikasi yang baik dengan kompleksitas komputasi yang tetap efisien. Penggunaan dua *hidden layer* pada LSTM memungkinkan model menangkap pola temporal trafik jaringan tanpa menambahkan *convolution layer* yang dapat meningkatkan kompleksitas parameter dan waktu komputasi. Penilaian model dicapai dengan menggunakan beberapa metrik, yakni akurasi, presisi, *recall,* serta *F1-score*. Perhitungan metrik evaluasi dilakukan menggunakan Persamaan (2) hingga Persamaan (5) berikut:

$$Accuracy = \frac{TP+TN}{TP+TN+FP+FN} \quad (2)$$

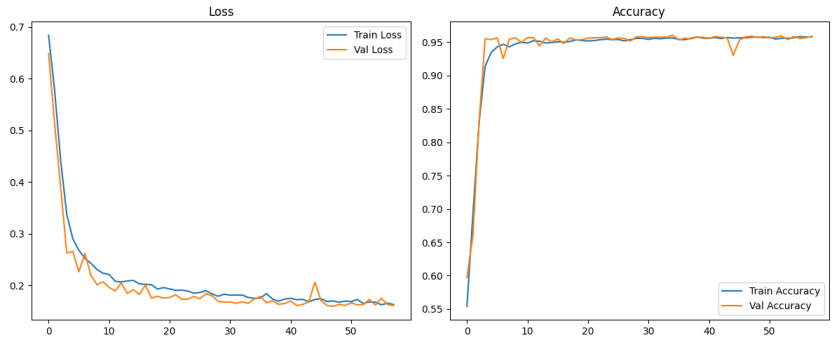
$$Precision = \frac{TP}{TP+FP} \quad (3)$$

$$Recall = \frac{TP}{TP+FN} \quad (4)$$

$$F1 = 2 \times \frac{Precision \times Recall}{Precision+Recall} \quad (5)$$

3. HASIL DAN PEMBAHASAN

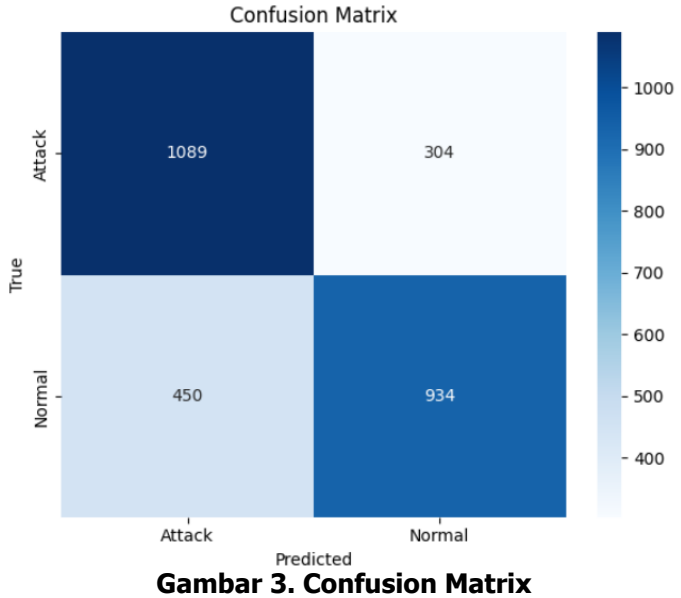
Hasil eksperimen diperoleh dari data uji sebesar 20% dari total dataset yang dipisahkan menggunakan metode *train-test split*. Model *Long Short-Term Memory* (LSTM) yang diusulkan menunjukkan performa yang baik dalam mendeteksi aktivitas botnet pada jaringan *Internet of Things* (IoT). Proses pelatihan model ditunjukkan pada grafik perubahan nilai *loss* dan *accuracy* pada Gambar 2. Grafik tersebut menunjukkan bahwa model mengalami konvergensi yang stabil selama proses pelatihan tanpa indikasi *overfitting* yang signifikan.



Gambar 2. *Loss* dan *Accuracy* Model

Dari hasil pengujian, model memperoleh akurasi sebesar 95,89% dan nilai *Area Under Curve* (AUC) sebesar 0,97. Nilai ini menunjukkan bahwa model memiliki kapabilitas klasifikasi yang

sangat baik dalam membedakan antara trafik yang normal dan serangan *botnet*. Visualisasi *confusion matrix* dapat dilihat pada Gambar 3.



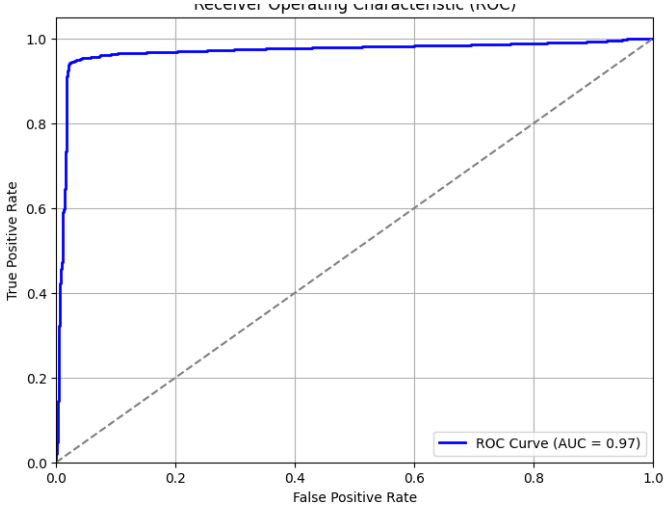
Gambar 3. Confusion Matrix

Untuk memberikan gambaran *numerik* yang lebih jelas, *confusion matrix* juga disajikan dalam bentuk tabel pada Tabel 5.

Tabel 5. *Confusion Matrix*

Predicted	***Attack***	**Normal**
Actual Attack	1357	36
Actual Normal	78	1306

Berdasarkan *confusion matrix* pada Tabel 4, jumlah *false negative* yang diperoleh relatif rendah, yaitu sebanyak 36 data. Hal ini menunjukkan bahwa model memiliki sensitivitas yang tinggi dalam mengenali pola serangan *botnet*. Dalam konteks keamanan jaringan IoT, nilai *false negativ*e yang rendah sangat penting karena serangan yang tidak terdeteksi dapat menyebabkan gangguan layanan maupun kompromi perangkat secara luas. Selain itu, jumlah *false positive* sebanyak 78 data menunjukkan bahwa sebagian kecil trafik normal masih diklasifikasikan sebagai serangan. Kondisi ini dapat disebabkan oleh kemiripan pola komunikasi antara trafik normal dengan aktivitas botnet tertentu, terutama pada trafik dengan *packet rate* tinggi. Meskipun demikian, nilai *precision* yang tinggi menunjukkan bahwa model tetap mampu mempertahankan stabilitas klasifikasi. Kombinasi nilai *precision* dan *recall* yang tinggi menghasilkan *F1-score* yang baik, sehingga menunjukkan bahwa model mampu menjaga keseimbangan performa dalam mendeteksi trafik normal maupun serangan *botnet*. Perhitungan metrik evaluasi dilakukan berdasarkan Persamaan (2)–(5).Kurva ROC yang menggambarkan performa klasifikasi model ditunjukkan pada Gambar 4. Kurva tersebut memperlihatkan bahwa model memiliki kemampuan diskriminasi yang sangat baik antara kelas normal dengan serangan.



Gambar 4. Grafik ROC

Secara karakteristik, trafik botnet pada dataset Bot-IoT memiliki pola temporal seperti peningkatan jumlah paket dalam interval waktu tertentu serta aktivitas komunikasi yang berulang. Dengan memanfaatkan arsitektur LSTM yang mampu menangkap dependensi temporal dalam data sekuensial, model dapat mengenali pola tersebut secara efektif. Hal ini menjadi keunggulan utama dibandingkan metode klasifikasi tradisional yang tidak mempertimbangkan urutan waktu.

Untuk memperkuat hasil penelitian, dilakukan perbandingan dengan beberapa metode pada penelitian sebelumnya yang ditunjukkan pada Tabel 6

Tabel 6. Perbandingan Metode Deteksi Botnet

Penelitian	Metode	Accuracy
Alkahtani & Aldhyani (2021)	CNN-LSTM	94%
Hasas et al. (2024)	LSTM + RF	95%
Hussain et al. (2025)	CNN-LSTM	95.5%
Penelitian ini	LSTM	95.89%

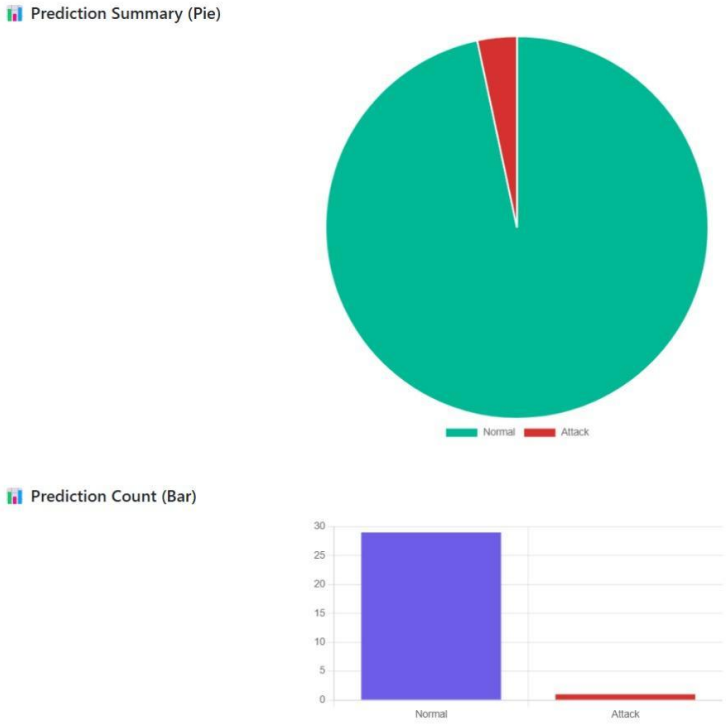
Hasil tersebut menunjukkan bahwa model LSTM yang diusulkan mampu memberikan performa yang kompetitif dibandingkan metode lain, bahkan dengan arsitektur yang lebih sederhana. Hal ini menunjukkan bahwa LSTM tidak hanya efektif dalam menangkap pola temporal, tetapi juga lebih efisien dari sisi kompleksitas komputasi sehingga lebih sesuai untuk implementasi pada perangkat IoT yang memiliki keterbatasan sumber daya. Namun demikian, terdapat beberapa keterbatasan dalam penelitian ini. Dataset yang digunakan masih berbasis simulasi sehingga belum sepenuhnya merepresentasikan kondisi jaringan IoT nyata. Selain itu, variasi serangan yang digunakan masih terbatas, sehingga diperlukan penelitian lanjutan dengan dataset yang lebih beragam.

Secara keseluruhan, hasil dari penelitian ini menunjukan bahwa model LSTM memiliki potensi yang sangat baik untuk diterapkan sebagai sistem deteksi botnet pada lingkungan IoT, khususnya pada sistem yang membutuhkan efisiensi komputasi. Selain evaluasi performa model, penelitian ini juga mengimplementasikan model deteksi botnet ke dalam sebuah aplikasi berbasis web menggunakan *framework Flask*. Aplikasi ini dirancang untuk

mempermudah pengguna dalam melakukan analisis trafik jaringan secara praktis melalui antarmuka yang sederhana.

Gambar 5. Form Upload Data IoT

Antarmuka ini memungkinkan pengguna untuk mengunggah dataset trafik jaringan dalam format CSV. Sistem kemudian akan memproses data menggunakan model LSTM yang telah dilatih sebelumnya untuk melakukan klasifikasi trafik.



Gambar 6. Dashboard Hasil Prediksi

Hasil klasifikasi ditampilkan dalam bentuk visualisasi grafik seperti pie chart dan bar chart yang menunjukkan perbandingan antara trafik normal dan serangan *botnet.* Visualisasi ini membantu pengguna dalam memahami hasil analisis secara lebih intuitif.

4. KESIMPULAN

Penelitian ini berhasil mengimplementasikan model *Long Short-Term Memory* (LSTM) untuk mendeteksi aktivitas botnet pada jaringan *Internet of Things* (IoT) berdasarkan analisis trafik jaringan. Model yang diusulkan mampu menangkap pola temporal dalam data sekuensial sehingga dapat membedakan antara trafik normal dan serangan *botnet* secara efektif. Hasil evaluasi menunjukkan bahwa model mencapai akurasi pada angka 95,89% dengan nilai AUC sebesar 0,97, yang menandakan performa klasifikasi yang sangat baik. Nilai *recall* yang tinggi

menunjukkan bahwa model dapat mendeteksi sebagian besar serangan botnet, sedangkan nilai *precision* yang tinggi menunjukkan kemampuan dalam mereduksi kesalahan klasifikasi terkait trafik normal. Dibandingkan dengan metode lain seperti CNN-LSTM, model LSTM yang digunakan dalam penelitian ini memiliki kompleksitas yang lebih rendah namun tetap mampu memberikan performa yang kompetitif. Hal ini menunjukkan bahwa pendekatan LSTM lebih sesuai untuk diterapkan pada lingkungan IoT yang memiliki keterbatasan sumber daya. Selain itu, implementasi model dalam bentuk aplikasi berbasis web menunjukkan bahwa sistem deteksi *botnet* dapat diterapkan secara praktis untuk mendukung proses analisis trafik jaringan secara semi *real-time*. Penelitian ini tetap memiliki batasan terkait dengan pemanfaatan dataset yang berbentuk simulasi serta variasi serangan yang kurang beragam. Oleh karena itu, disarankan agar studi yang akan datang menggunakan dataset yang lebih bervariasi, menguji model pada lingkungan IoT nyata, serta mengeksplorasi arsitektur lain seperti CNN-LSTM atau *Transformer* untuk meningkatkan kinerja deteksi.

DAFTAR RUJUKAN

Agus Syamsul Arifin, M., Anto Tri Susilo, A., Taqwa Martadinata, A., & Santoso, B. (2024). Deteksi Aktifitas Malware pada Internet of Things menggunakan Algoritma Decision Tree dan Random Forest. *Media Online)*, *4*(6), 3073–3079. https://doi.org/10.30865/klik.v4i6.1903

Alkahtani, H., & Aldhyani, T. H. H. (2021). Botnet Attack Detection by Using CNN-LSTM Model for Internet of Things Applications. *Security and Communication Networks*, *2021*. https://doi.org/10.1155/2021/3806459

Almousa, O., Hamdallh, B., & Al-Nu'man, R. (2025). Enhancing IoT Security: A Comparative Analysis of Machine Learning and Deep Learning Techniques for Botnet Detection. *Engineering, Technology and Applied Science Research*, *15*(4), 24498–24505. https://doi.org/10.48084/etasr.11092

Ashiku, L., & Dagli, C. (2021). Network Intrusion Detection System using Deep Learning. *Procedia Computer Science*, *185*(June), 239–247. https://doi.org/10.1016/j.procs.2021.05.025

Efendi, R., Wahyono, T., & Widiasari, I. R. (2024). DBSCAN SMOTE LSTM: Effective Strategies for Distributed Denial of Service Detection in Imbalanced Network Environments. *Big Data and Cognitive Computing*, *8*(9). https://doi.org/10.3390/bdcc8090118

Hadiningrum, T. R., Talasari, R. A. D., Ilham, K. F., & Ijtihadie, R. M. (2025). Survey on Risks Cyber Security in Edge Computing for The Internet of Things Understanding Cyber Attacks Threats and Mitigation. In *JUTI: Jurnal Ilmiah Teknologi Informasi* (pp. 29–50). https://doi.org/10.12962/j24068535.v23i1.a1210

Hasas, A., Zarinkhail, M. S., Hakimi, M., & Quchi, M. M. (2024). Strengthening Digital Security: Dynamic Attack Detection with LSTM, KNN, and Random Forest. *Journal of Computer*

Science and Technology Studies, *6*(1), 49–57. https://doi.org/10.32996/jcsts.2024.6.1.6

Hezam, A. A., Mostafa, S. A., Baharum, Z., Alanda, A., & Salikon, Z. (2021). *INTERNATIONAL JOURNAL ON INFORMATICS VISUALIZATION journal homepage : www.joiv.org/index.php/joiv INTERNATIONAL JOURNAL ON INFORMATICS VISUALIZATION Combining Deep Learning Models for Enhancing the Detection of Botnet Attacks in Multiple Sensors Internet* . *5*(December), 380–387. www.joiv.org/index.php/joiv

Hussain, O. A., Chen, Z., & Zhu, H. (2025). sSecure Net: A Hybrid CNN-LSTM-based Intrusion Detection System for Securing IoT Networks. *Proceedings of the 4th International Conference on Computer, Artificial Intelligence and Control Engineering, CAICE 2025*, 537–544. https://doi.org/10.1145/3727648.3727736

Hussan, M. I. T., Reddy, G. V., Anitha, P. T., Kanagaraj, A., & Naresh, P. (2024). DDoS attack detection in IoT environment using optimized Elman recurrent neural networks based on chaotic bacterial colony optimization. *Cluster Computing*, *27*(4), 4469–4490. https://doi.org/10.1007/s10586-023-04187-4

Kartadie, R., Kusjani, A., Kusnanto, Y., & Harnaningrum, L. N. (2025). Optimizing LSTM-CNN for Lightweight and Accurate DDoS Detection in SDN Environments. *Scientific Journal of Informatics*, *12*(2), 295–310. https://doi.org/10.15294/sji.v12i2.24531

Muhammad Al Adib, Pebruarianto Hutabarat, Heru Fredi, Bill Raj, Prasetyo, & Empiter Gea. (2025). Evaluasi Kinerja CNN, LSTM, dan DNN untuk Deteksi Serangan DDoS Berbasis Flow features pada Dataset CSE-CIC-IDS2018. *Jurnal Komputer Teknologi Informasi Sistem Informasi (JUKTISI)*, *4*(3), 1639–1649. https://doi.org/10.62712/juktisi.v4i3.727

Priyambodo, B., Ghozi, W., & Rafrastara, F. A. (2026). Optimasi Kinerja Sistem Deteksi Intrusi Menggunakan Hybrid Xgboost Dan Arsitektur Deep Learning Efisien. *Rabit : Jurnal Teknologi Dan Sistem Informasi Univrab*, *11*(1), 919–933. https://doi.org/10.36341/rabit.v11i1.7182

Syaikhurrahman, M., & Prasetyo, B. (2025). *DETEKSI SERANGAN DDOS MENGGUNAKAN DEEP LEARNING DALAM ADMINISTRASI JARINGAN karena memberikan strategi preventif untuk melindungi infrastruktur fisik dan perangkat mesin . Deep learning dapat dijadikan bagian integral dari keamanan jaringan karena dihubun*. *6*(6), 8995–9003.

Wazzan, M., Algazzawi, D., Bamasaq, O., Albeshri, A., & Cheng, L. (2021). Internet of things botnet detection approaches: Analysis and recommendations for future research. *Applied Sciences (Switzerland)*, *11*(12). https://doi.org/10.3390/app11125713

Zahid, M., & Bharati, T. S. (2025). Enhancing cybersecurity in IoT systems: a hybrid deep

learning approach for real-time attack detection. In *Discover Internet of Things* (Vol. 5, Issue 1). Springer International Publishing. ttps://doi.org/10.1007/s43926-025-00156-y