202010370311414
Padang Ikhrosim
Prodi Informatika

DETEKSI SERANGAN LRDDOS MENGGUNAKAN ENSEMBLE STACKING DENGAN KNN DAN XGBOOST.

Laporan Tugas Akhir

Diajukan Untuk Memenuhi Persyaratan

Guna Meraih Gelar Sarjana Strata 1

Informatika Universitas Muhammadiyah Malang

Padang ikhrosim

202010370311414

Bidang Minat

Jaringan

PROGRAM STUDI INFORMATIKA

FAKULTAS TEKNIK

UNIVERSITAS MUHAMMADIYAH MALANG

2026

202010370311414
Padang Ikhrosim
Prodi Informatika

LEMBAR PERSETUJUAN

Deteksi Serangan LRDDoS Menggunakan Ensemble Stacking Dengan KNN dan XGBoost

TUGAS AKHIR

Sebagai Persyaratan Guna Meraih Gelar Sarjana Strata 1
Informatika Universitas Muhammadiyah Malang

Menyetujui,

Malang, 20 April 2026

Dosen Pembimbing 1	Dosen Pembimbing 2
Dr. Diah Risqiwati ST., MT.	**Ir Denar Regata Akbi S.Kom., M.Kom.**
NIP. 10814100545PNS.	**NIP. 10816120591PNS.**

202010370311414
Padang Ikhrosim
Prodi Informatika

LEMBAR PENGESAHAN

Deteksi Serangan LRDDoS Menggunakan Ensemble Stacking Dengan KNN dan XGBoost.

TUGAS AKHIR

Sebagai Persyaratan Guna Meraih Gelar Sarjana Strata 1
Informatika Universitas Muhammadiyah Malang

Disusun oleh :

Padang Ikhrosim

202010370311414

Tugas Akhir ini telah diuji dan dinyatakan lulus melalui sidang majelis penguji pada tanggal 20 April 2026

Menyetujui,

Dosen Pembimbing 1	Dosen Pembimbing 2
Dr. Diah Risqiwati ST., MT.	**Ir Denar Regata Akbi S.Kom., M.Kom.**
NIP. 10814100545PNS.	**NIP. 10816120591PNS.**

Dosen Penguji 1	Dosen Penguji 2
Ir. Mahar Faiqurahman S.Kom., M.T.	**Ir. Syaifuddin S.Kom., M.Kom., IPM, ASEAN Eng**
NIP. 10808110462PNS.	**NIP. 10816120590PNS.**

Mengetahui,
Ketua Jurusan Informatika

Ir. Agus Eko Minarno S.Kom., M.Kom. IPM.
NIP. 10814100540PNS.

202010370311414
Padang Ikhrosim
Prodi Informatika

LEMBAR PERNYATAAN

Yang bertanda tangaan dibawah ini :

NAMA : **PADANG IKHROSIM**

NIM : **202010370311414**

FAK/JUR : **TEKNIK / INFORMATIKA**

Dengan ini saya menyatakan bahwa Tugas Akhir dengan judul "**Deteksi Serangan LRDDoS Menggunakan Ensemble Stacking Dengan KNN dan XGBoost.** " beserta seluruh isinya adalah karya saya sendiri dan bukan merupakan karya tulis orang lain, baik sebagian maupun seluruhnya, kecuali dalam bentuk kutipan yang telah disebutkan sumbernya.

Demikian surat pernyataan ini saya buat dengan sebenar – benarnya. Apabila kemudian hari ditemukan adanya pelanggaran terhadap etika keilmuan dalam karya saya ini, atau ada klaim dari pihak lain terhadap keaslian karya saya ini, maka saya siap menanggung segala bentuk resiko/sanksi yang berlaku.

Mengetahui,
Dosen Pembimbing

Dr. Diah Risqiwati ST., MT.

Malang, 20 April 2026
Yang Membuat Pernyataan

Padang Ikhrosim

202010370311414
Padang Ikhrosim
Prodi Informatika

ABSTRAK

Serangan ***Low-Rate Distributed Denial of Service*** **(LRDDoS)** merupakan salah satu bentuk serangan DDoS yang sulit dideteksi karena pola lalu lintasnya menyerupai trafik normal namun dilakukan secara terus-menerus untuk mengganggu kinerja jaringan. Pada lingkungan *Software-Defined Internet of Things* (SD-IoT), serangan ini dapat berdampak signifikan terhadap ketersediaan layanan karena arsitektur jaringan yang terpusat pada *controller*. Penelitian ini bertujuan untuk menganalisis performa algoritma ***K-Nearest Neighbors*** **(KNN),** ***Extreme Gradient Boosting*** **(XGBoost)**, dan metode ***Ensemble Stacking*** dalam mendeteksi serangan LRDDoS pada jaringan SD-IoT. Dataset yang digunakan berjumlah 200.000 data yang terdiri dari 160.006 data latih dan 39.994 data uji, dengan 22 fitur yang diekstraksi dari lalu lintas jaringan. Pengujian dilakukan pada tiga skenario *packet per second* (pps), yaitu 20pps, 50pps, dan 70pps. Parameter evaluasi yang digunakan meliputi *accuracy, precision, recall, F1-score,* dan *predict loss*. Hasil penelitian menunjukkan bahwa algoritma KNN memiliki performa yang relatif rendah dan stabil di sekitar 50% pada seluruh skenario pengujian. XGBoost menunjukkan performa terbaik pada skenario 50pps dengan akurasi di atas 90%, serta keseimbangan nilai precision dan recall yang baik. Metode *Ensemble Stacking* menghasilkan akurasi sebesar 87,519% pada 20pps, namun mengalami penurunan performa pada 50pps dan 70pps. Berdasarkan hasil tersebut, XGBoost merupakan algoritma yang paling konsisten dalam mendeteksi serangan LRDDoS pada kondisi yang diuji, sedangkan metode stacking memberikan peningkatan performa pada trafik rendah namun belum stabil pada trafik yang lebih tinggi.

Kata kunci: LRDDoS, SD-IoT, KNN, XGBoost, Ensemble Stacking, Machine Learning.

202010370311414
Padang Ikhrosim
Prodi Informatika

ABSTRACT

Low-Rate Distributed Denial of Service (LRDDoS) attacks are a form of DDoS attacks that are difficult to detect due to their traffic patterns resembling normal network behavior while continuously disrupting network performance. In a Software-Defined Internet of Things (SD-IoT) environment, such attacks can significantly affect service availability due to the centralized controller-based architecture. This study aims to analyze the performance of **K-Nearest Neighbors (KNN)**, **Extreme Gradient Boosting (XGBoost)**, and **Ensemble Stacking** methods in detecting LRDDoS attacks within an SD-IoT network. The dataset used in this study consists of 200,000 records, including 160,006 training data and 39,994 testing data, with 22 extracted network traffic features. The evaluation was conducted under three packet per second (pps) scenarios: 20pps, 50pps, and 70pps. Performance metrics used in this study include accuracy, precision, recall, F1-score, and predict loss. The results indicate that the KNN algorithm achieved relatively low and stable performance around 50% accuracy across all scenarios. XGBoost demonstrated the best performance at 50pps, achieving accuracy above 90% with balanced precision and recall values. The Ensemble Stacking method achieved 87.519% accuracy at 20pps but experienced performance degradation at 50pps and 70pps. Based on these findings, XGBoost is the most consistent algorithm for detecting LRDDoS attacks under the tested conditions, while the stacking method improves performance in low-traffic scenarios but lacks stability under higher traffic loads.

Keywords: LRDDoS, SD-IoT, KNN, XGBoost, Ensemble Stacking, Machine Learning.

202010370311414
Padang Ikhrosim
Prodi Informatika

KATA PENGANTAR

Puji syukur penulis panjatkan kepada Tuhan Yang Maha Esa atas segala rahmat dan karunia-Nya sehingga penulis dapat menyelesaikan skripsi ini dengan baik. Skripsi yang berjudul " Deteksi serangan LRDDoS menggunakan Ensemble Stacking dengan KNN dan XGBoost " ini disusun sebagai salah satu syarat untuk memperoleh gelar sarjana pada program studi Teknik Informatika, Universitas Muhammadiyah Malang. Proses penyusunan skripsi ini tentunya tidak terlepas dari do'a, dukungan, dan bantuan dari berbagai pihak yang telah memberikan kontribusi yang sangat berharga.

Penulis menyampaikan terima kasih yang sebesar-besarnya kepada Ibu Dr. Diah Risqiwati ST., MT. selaku dosen pembimbing I dan Bapak Ir. Denar Regata Akbi S.Kom., M.Kom. selaku dosen pembimbing II yang telah meluangkan waktu, tenaga, serta pikiran untuk memberikan arahan, bimbingan, dan masukan yang sangat berarti selama penyusunan skripsi ini. Ucapan terima kasih juga penulis sampaikan kepada orang tua tercinta atas do'a, kasih sayang, dan dukungan yang tiada henti, serta kepada semua pihak yang telah membantu

202010370311414
Padang Ikhrosim
Prodi Informatika

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

202010370311414
Padang Ikhrosim
Prodi Informatika

DAFTAR RUMUS

DAFTAR PUSTAKA

[1] M. K. Harto and A. Basuki, “Deteksi Serangan DDoS Pada Jaringan Berbasis SDN Dengan Klasifikasi Random Forest,” 2021. [Online]. Available: http://j-ptiik.ub.ac.id

[2] B. Nugraha and R. N. Murthy, “Deep Learning-based Slow DDoS Attack Detection in SDN-based Networks,” in *2020 IEEE Conference on Network Function Virtualization and Software Defined Networks, NFV-SDN 2020 - Proceedings*, Institute of Electrical and Electronics Engineers Inc., Nov. 2020, pp. 51–56. doi: 10.1109/NFV-SDN50289.2020.9289894.

[3] N. Sugianti, Y. Galuh, S. Fatia, and K. F. H. Holle, “Deteksi Serangan Distributed Denial of Services (DDOS) Berbasis HTTP Menggunakan Metode Fuzzy Sugeno,” 2020.

[4] F. Antony and R. Gustriansyah, “Deteksi Serangan Denial of Service pada Internet of Things Menggunakan Finite-State Automata,” *MATRIK : Jurnal Manajemen, Teknik Informatika dan Rekayasa Komputer*, vol. 21, no. 1, pp. 43–52, Nov. 2021, doi: 10.30812/matrik.v21i1.1078.

[5] A. Harris, A. Rahim, S. Komputer, and S. Dinamika Bangsa, “Seleksi Fitur dengan Information Gain untuk Meningkatkan Deteksi Serangan DDoS Menggunakan Random Forest An Information Gain Feature Selection to Improve DDoS Detection using Random Forest.”

[6] P. Bhale, S. Biswas, and S. Nandi, “Low Rate DDoS Attack Detection and Mitigation Using Lightweight Distributed Packet Inspection Agent in IoT Ecosystem,” in *International Symposium on Advanced Networks and Telecommunication Systems, ANTS*, IEEE Computer Society, Dec. 2019. doi: 10.1109/ANTS47819.2019.9118052.

[7] A. M. Nair and R. Santhosh, “Two Phase Detection Process to Mitigate LRDDoS Attack in Cloud Computing Environment.” [Online]. Available: www.ijacsa.thesai.org

[8] H. Cheng, J. Liu, T. Xu, B. Ren, J. Mao, and W. Zhang, “Machine learning based low-rate DDoS attack detection for SDN enabled IoT networks,” 2020.

[9] M. Baskar, J. Ramkumar, C. Karthikeyan, V. Anbarasu, A. Balaji, and T. S. Arulananth, “Low rate DDoS mitigation using real-time multi threshold traffic monitoring system,” *J. Ambient Intell. Humaniz. Comput.*, 2021, doi: 10.1007/s12652-020-02744-y.

[10] A. Irfani, N. Iman, F. Dwi Sumadi, and Z. Sari, "Low Rate DDOS Attack Detection Using KNN On SD-IOT," *REPOSITOR*, vol. 5, no. 1, pp. 603–608, 2023.

[11] W. D. Nanda and F. D. S. Sumadi, "LRDDoS Attack Detection on SD-IoT Using Random Forest with Logistic Regression Coefficient," *Jurnal RESTI*, vol. 6, no. 2, pp. 220–226, Apr. 2022, doi: 10.29207/resti.v6i2.3878.

[12] F. D. S. Sumadi and C. S. K. Aditya, "Comparative Analysis of DDoS Detection Techniques Based on Machine Learning in OpenFlow Network," in *2020 3rd International Seminar on Research of Information Technology and Intelligent Systems (ISRITI)*, IEEE, Dec. 2020, pp. 1–1. doi: 10.1109/ISRITI51436.2020.9315352.

[13] M. Abizar, M. F. S. I. Syahputra, A. R. Habibullah, C. S. K. Aditya, and F. D. S. Sumadi, "Low-rate distributed denial of service attacks detection in software defined network-enabled internet of things using machine learning combined with feature importance," *IAES International Journal of Artificial Intelligence*, vol. 12, no. 4, pp. 1974–1984, Dec. 2023, doi: 10.11591/ijai.v12.i4.pp1974-1984.

[14] S. R. Awad, Q. I. Ali, and A. I. Daood, "Journal of Engineering and Technology for Industrial Applications ITEGAM-JETIA SECURE AND INTELLIGENT SDN ROUTING AND ANOMALY DETECTION USING XG-BOOST FOR REAL-TIME IOT TRAFFIC OPTIMIZATION", doi: 10.5935/jetia.

[15] F. Sumadi, "LRDDoS Dataset (CoAP)," Mendeley Data.

[16] A. Pakmehr, A. Aßmuth, N. Taheri, and A. Ghaffari, "DDoS attack detection techniques in IoT networks: a survey," *Cluster Comput.*, vol. 27, no. 10, pp. 14637–14668, Dec. 2024, doi: 10.1007/s10586-024-04662-6.

[17] D. Cahyanti, A. Rahmayani, and S. Ainy Husniar, "Indonesian Journal of Data and Science Analisis performa metode Knn pada Dataset pasien pengidap Kanker Payudara," vol. 1, no. 2, pp. 39–43, 2020.

[18] R. Harahap, M. Irpan, M. Azzuhri Dinata, and L. Efrizoni, "PERBANDINGAN ALGORITMA RANDOM FOREST DAN XGBOOST UNTUK KLASIFIKASI PENYAKIT PARU-PARU BERDASARKAN DATA DEMOGRAFI PASIEN," 2024.

[19] D. Djafar Sidik and D. Tjong Wan Sen, "Penggunaan Stacking Classifier Untuk Prediksi Curah Hujan," *IT FOR SOCIETY*, vol. 04, no. 01.

[20] S. K. Keshari, V. Kansal, and S. Kumar, "A Systematic Review of Quality of Services (QoS) in Software Defined Networking (SDN)," *Wirel. Pers. Commun.*, vol. 116, no. 3, pp. 2593–2614, Feb. 2021, doi: 10.1007/s11277-020-07812-2.

[21] S. Bhardwaj and S. N. Panda, "Performance Evaluation Using RYU SDN Controller in Software-Defined Networking Environment," *Wirel. Pers. Commun.*, vol. 122, no. 1, pp. 701–723, Jan. 2022, doi: 10.1007/s11277-021-08920-3.

[22] R. Wazirali, R. Ahmad, and S. Alhiyari, "Sdn-openflow topology discovery: An overview of performance issues," Aug. 01, 2021, *MDPI AG*. doi: 10.3390/app11156999.

[23] D. Y. Setiawan, S. N. Hertiana, and R. M. Negara, "6LoWPAN Performance Analysis of IoT Software-Defined-Network-Based Using Mininet-Io," in *IoTaIS 2020 - Proceedings: 2020 IEEE International Conference on Internet of Things and Intelligence Systems*, Institute of Electrical and Electronics Engineers Inc., Jan. 2021, pp. 60–65. doi: 10.1109/IoTaIS50849.2021.9359714.

[24] L. H. Chang, T. H. Lee, H. C. Chu, and C. W. Su, "Application-Based Online Traffic Classification with Deep Learning Models on SDN Networks," *Advances in Technology Innovation*, vol. 5, no. 4, pp. 216–229, Sep. 2020, doi: 10.46604/aiti.2020.4286.

[25] A. Muhammad, A. Rudianto, E. Sakti Pramukantoro, and D. Kurnianingtyas, "Implementasi Sistem Deteksi Anomali pada Jaringan Komputer dengan Pendekatan XGBoost dan Data SNMP," 2025. [Online]. Available: http://j-ptiik.ub.ac.id

FORM CEK PLAGIARISME LAPORAN TUGAS AKHIR

Nama Mahasiswa : **PADANG IKHROSIM**

NIM : **202010370311414**

Judul TA : **DETEKSI SERANGAN LRDDOS MENGGUNAKAN ENSEMBLE STACKING DENGAN KNN DAN XGBOOST**

Hasil Cek Plagiarisme dengan Turnitin

No.	Komponen Pengecekan	Nilai Maksimal Plagiarisme (%)	Hasil Cek Plagiarisme (%) *
1.	Bab 1 – Pendahuluan	10 %	10%
2.	Bab 2 – Daftar Pustaka	25 %	19%
3.	Bab 3 – Analisis dan Perancangan	25 %	8%
4.	Bab 4 – Implementasi dan Pengujian	15 %	0%
5.	Bab 5 – Kesimpulan dan Saran	5 %	4%
6.	Makalah Tugas Akhir	20%	7%

) Hasil cek plagiarism diisi oleh pemeriksa (staf TU)

***) Maksimal 5 kali (4 Kali sebelum ujian, 1 kali sesudah ujian)**

Mengetahui,

Pemeriksa (Staff TU)

UNIVERSITAS MUHAMMADIYAH MALANG
FAKULTAS TEKNIK

(.....)