Digital Transformation Technology (Digitech) | e-ISSN: 2807-9000
Volume 6, **Number** 1, Maret 2026
https://doi.org/10.47709/digitech.v6i1.9050

Implementasi Sistem Keamanan Server Berbasis AI Menggunakan Algoritma Extreme Gradient Boosting (XGBoost) pada Debian 12

Roito Kasta Nadia Siahaan[1*], Firman Torino Sianturi[2], Reyfan Sibagariang[3], Lotar Mateus Sinaga[4].
[1,2,3,4]Universitas Katolik Santo Thomas,Medan
[1]roitosiahaan1@gmail.com, [2]firmansianturi354@gmail.com, [3]reyfansibagariang882@gmail.com, [4]lotarmateus88@gmail.com

open access
Histori Artikel:
Diajukan: 30 Juni 2026
Disetujui: 27 Juli 2026
Dipublikasi: 27 Juli 2026
Kata Kunci:
Intrusion Detection System; XGBoost; Machine Learning; Keamanan Jaringan; Artificial Intelligence; Serangan Siber

Digital Transformation Technology (Digitech) *is an Creative Commons License This work is licensed under a Creative Commons Attribution-NonCommercial 4.0 International (CC BY-NC 4.0).*

Abstrak
Ancaman keamanan siber seperti Distributed Denial of Service (DDoS) dan Brute Force terus mengalami peningkatan yang signifikan mengancam integritas dan ketersediaan layanan server berbasis jaringan.Penedekataan konvensional menggunakan firewall statis dan sistem aturan berbasis tanda tangan (signature-based) dinilai kurang efektif dalam menghadapi pola serangan yang semakin kompleks dan adaptif.Penelitian ini bertujuan untuk merancang dan mengimplementasikan sistem keamanan server berbasis kecerdasan buatan (Artifical Intelligence/AI) menggunakan algoritma Extreme Gradient Boosting (XGBoost) pada lingkungan sistem operasi Debian 12. Metode yang digunakan meliputi pembuatan dataset simulasi trafik jaringan yang mencerminkan kondisi normal, serangan DDoS, dan serangan Brute Force, diikuti dengan pelatihan model machine learning menggunakan Pustaka XGBoost pada lingkungan Python virtual environment. Model dilatih menggunakan tiga fitur utama: packet rate per detik, byte rate (KB), dan jumlah koneksi gagal. Implementasi dilakukan pada platform VirtualBox dengan Debian 12 sebagai sistem operasi host. Hasil pengujian menunjukkan bahwa model XGBoost yang dikembangkan berhasil mencapai akurasi klasifikasi sebesar 99,50%, dengan kemampuan mendeteksi serangan DDoS dan Brute Force secara real-time. Sistem mampu mengklasifikasikan trafik jaringan ke dalam kategori normal atau berbahaya dengan keyakinan di atas 99%, serta secara otomatis mengaktifkan mekanisme perlindungan firewall ketika serangan terdeteksi. Penelitian ini membuktikan bahwa pendekatan machine learning berbasis XGBoost merupakan solusi yang efektif, efisien, dan skalabel untuk implementasi Intrusion Detection System (IDS) pada lingkungan server modern.

PENDAHULUAN

Pesatnya kemajuan teknologi informasi meningkatkan ketergantungan organisasi, perusahaan, dan individu pada infrastruktur jaringan komputer. Hal ini memicu lonjakan ancaman siber yang signifikan dari segi frekuensi, kompleksitas, dan dampaknya. Menurut laporan Cybersecurity Ventures (2023), kerugian akibat kejahatan siber diproyeksikan mencapai 10,5 triliun dolar AS per tahun pada tahun 2025, sehingga keamanan jaringan kini menjadi prioritas utama dalam tata kelola TI modern.

Dua jenis serangan yang paling umum dan merugikan bagi infrastruktur server adalah *Distributed Denial of Service* (DDoS) dan *Brute Force*. Serangan DDoS bertujuan membanjiri server dengan trafik masif agar layanan tidak dapat diakses pengguna sah, sedangkan *Brute Force* mencoba berbagai kombinasi kredensial secara sistematis untuk mendapat akses ilegal. Agrawal et al. (2022) menyatakan bahwa kedua serangan ini dapat menyebabkan *downtime*, kebocoran data sensitif, kerugian finansial, dan kerusakan reputasi yang serius.

Pendekatan konvensional seperti firewall statis dan *signature-based* IDS memiliki keterbatasan besar. Sistem berbasis tanda tangan hanya efektif melawan serangan yang sudah dikenal dan gagal mendeteksi ancaman baru atau variasi pola belum terdokumentasi. Keterbatasan ini mendorong pengembangan solusi yang lebih adaptif dan cerdas menggunakan Kecerdasan Buatan (*Artificial Intelligence*/AI) dan Pembelajaran Mesin (*Machine Learning*/ML).

Algoritma *Extreme Gradient Boosting* (XGBoost) merupakan metode *machine learning* yang terbukti unggul karena dioptimalkan untuk kecepatan komputasi dan efisiensi memori. Algoritma ini berkinerja sangat baik dalam tugas klasifikasi biner maupun multikelas, termasuk deteksi anomali keamanan jaringan (Chen & Guestrin, 2023). Di sisi lain, Debian 12 ("Bookworm") adalah distribusi Linux yang stabil dan aman untuk server produksi. Kombinasi stabilitas Debian 12 dan kemampuan AI XGBoost menawarkan solusi keamanan server yang cerdas dan responsif.

Berdasarkan latar belakang yang telah dipaparkan, rumusan masalah dalam penelitian ini adalah: (1) Bagaimana merancang dan mengimplementasikan sistem deteksi serangan jaringan berbasis AI dengan algoritma XGBoost pada Debian 12?(2) Bagaimana tingkat akurasi model XGBoost dalam mengklasifikasikan trafik normal, serangan DDoS, dan serangan Brute Force? (3) Bagaimana integrasi sistem deteksi dengan mekanisme respons otomatis firewall?

Tujuan penelitian ini adalah: (1) Mengimplementasikan sistem Intrusion Detection System (IDS) berbasis machine learning menggunakan algoritma XGBoost pada sistem operasi Debian 12; (2) Mengukur dan menganalisis kinerja model XGBoost dalam mendeteksi serangan jaringan; (3) Mengembangkan prototipe sistem keamanan server yang mampu mendeteksi dan merespons ancaman secara otomatis. Manfaat penelitian ini mencakup kontribusi akademik berupa referensi implementasi IDS berbasis AI, serta kontribusi praktis berupa prototipe sistem keamanan yang dapat diadaptasi untuk lingkungan server nyata.

STUDI LITERATUR

Kecerdasan Buatan (Artificial Intelligence)

Kecerdasan buatan (Artificial Intelligence/AI) merupakan cabang ilmu komputer yang berfokus pada pengembangan sistem yang mampu melakukan tugas-tugas yang membutuhkan kecerdasan manusia, seperti penalaran, pembelajaran, persepsi, dan pengambilan keputusan. Dalam konteks keamanan siber, AI diaplikasikan untuk menganalisis pola trafik jaringan, mendeteksi anomali, dan mengklasifikasikan jenis serangan secara otomatis (Russell & Norvig, 2022). Pendekatan AI telah terbukti lebih adaptif dibandingkan sistem berbasis aturan konvensional karena kemampuannya untuk belajar dari data baru dan mengidentifikasi ancaman yang belum pernah ditemui sebelumnya.

Extreme Gradient Boosting (XGBoost)

XGBoost (Extreme Gradient Boosting) adalah algoritma machine learning berbasis ensemble yang dikembangkan oleh Chen dan Guestrin (2016) dan telah menjadi salah satu algoritma paling populer dalam kompetisi data science. XGBoost membangun kumpulan pohon keputusan (decision trees) secara bertahap, di mana setiap pohon baru berusaha memperbaiki kesalahan prediksi dari pohon-pohon sebelumnya menggunakan teknik gradient boosting. Keunggulan utama XGBoost meliputi: kecepatan komputasi yang tinggi berkat implementasi paralel, kemampuan menangani nilai yang hilang (missing values), regularisasi bawaan untuk mencegah overfitting, dan portabilitas yang baik (Chen & Guestrin, 2023). Penelitian oleh Ullah et al. (2022) membuktikan bahwa XGBoost mencapai akurasi deteksi intrusi jaringan sebesar 99,7% pada dataset NSL-KDD, mengungguli algoritma Random Forest dan Support Vector Machine.

Keamanan Siber dan Ancaman DDoS

Distributed Denial of Service (DDoS) merupakan salah satu ancaman keamanan siber yang paling merusak, di mana penyerang menggunakan jaringan komputer yang telah dikompromi (botnet) untuk membanjiri target dengan volume trafik yang sangat besar. Serangan DDoS dapat menyebabkan layanan tidak tersedia selama berjam-jam hingga berhari-hari, mengakibatkan kerugian finansial yang sangat besar. Laporan Cloudflare (2024) mencatat peningkatan serangan DDoS sebesar 117% pada tahun 2023, dengan serangan volumetrik mencapai terabyte per detik. Karakteristik serangan DDoS yang terdeteksi melalui machine learning meliputi lonjakan packet rate, peningkatan bandwidth yang signifikan, dan distribusi sumber trafik yang tidak normal.

Serangan Brute Force

Serangan Brute Force adalah metode di mana penyerang mencoba semua kemungkinan kombinasi kata sandi atau kunci enkripsi secara sistematis untuk mendapatkan akses tidak sah ke sistem. Dalam konteks keamanan server, serangan Brute Force sering menargetkan layanan SSH, FTP, dan panel admin web. Karakteristik utama serangan Brute Force yang dapat dideteksi melalui analisis trafik meliputi: tingginya jumlah percobaan autentikasi yang gagal dalam periode waktu singkat, pola akses berulang dari sumber yang sama, dan regularitas temporal yang tidak alami. Model machine learning dapat mengidentifikasi pola ini secara efektif berdasarkan fitur-fitur statistik dari trafik jaringan (Jain & Kesswani, 2022).

Firewall sebagai Mekanisme Respons

Firewall adalah komponen keamanan jaringan yang memantau dan mengontrol lalu lintas jaringan berdasarkan aturan keamanan yang telah ditentukan. Dalam skenario IDS terintegrasi, firewall berperan sebagai mekanisme respons aktif yang secara otomatis memblokir atau membatasi trafik yang telah diidentifikasi sebagai ancaman oleh sistem deteksi. Integrasi antara IDS berbasis AI dan firewall yang responsif menciptakan sistem keamanan yang tidak hanya mampu mendeteksi ancaman, tetapi juga merespons secara otomatis dalam waktu

nyata (Ngo et al., 2023). Pada sistem operasi Linux termasuk Debian 12, iptables dan nftables merupakan alat firewall yang umum digunakan.

METODE

Jenis Penelitian

Penelitian ini merupakan penelitian terapan (applied research) dengan pendekatan eksperimental. Penelitian difokuskan pada perancangan, implementasi, dan evaluasi sistem keamanan server berbasis AI menggunakan algoritma XGBoost pada platform Debian 12. Metode penelitian mencakup studi literatur, perancangan sistem, implementasi teknis, pengujian, dan analisis hasil.

Lingkungan Penelitian

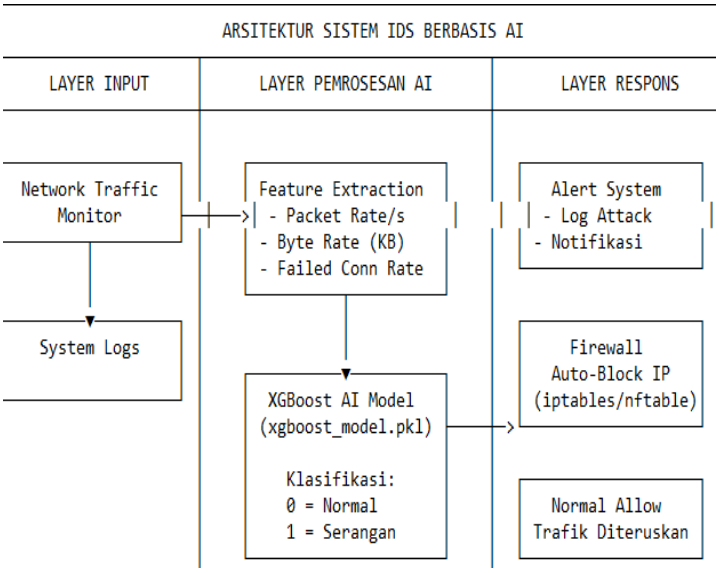
Implementasi sistem dilakukan pada lingkungan tervirtualisasi menggunakan VirtualBox sebagai hypervisor dengan Debian 12 sebagai sistem operasi tamu. Lingkungan virtual dipilih untuk memudahkan reproduksibilitas eksperimen, isolasi lingkungan pengujian, dan kemudahan dalam melakukan snapshot sistem. Spesifikasi lingkungan penelitian ditampilkan pada Tabel 1 dan Tabel 2.

Tabel 1. Spesifikasi Software yang Digunakan

Perangkat Lunak	Versi	Fungsi
Oracle VirtualBox	7.0+	Platform virtualisasi
Debian 12 "Bookworm"	12.x	Sistem operasi server
Python	3.11+	Bahasa pemrograman utama
XGBoost	1.7+	Algoritma machine learning
Scikit-learn	1.3+	Evaluasi model dan split data
NumPy	1.24+	Komputasi numerik array
Pandas	2.0+	Manipulasi dan analisis data
Pickle (built-in)	3.x	Serialisasi dan penyimpanan model

Arsitektur Sistem

Arsitektur sistem keamanan server berbasis AI yang dikembangkan terdiri atas beberapa komponen utama yang terintegrasi, sebagaimana ditampilkan pada Gambar 1.

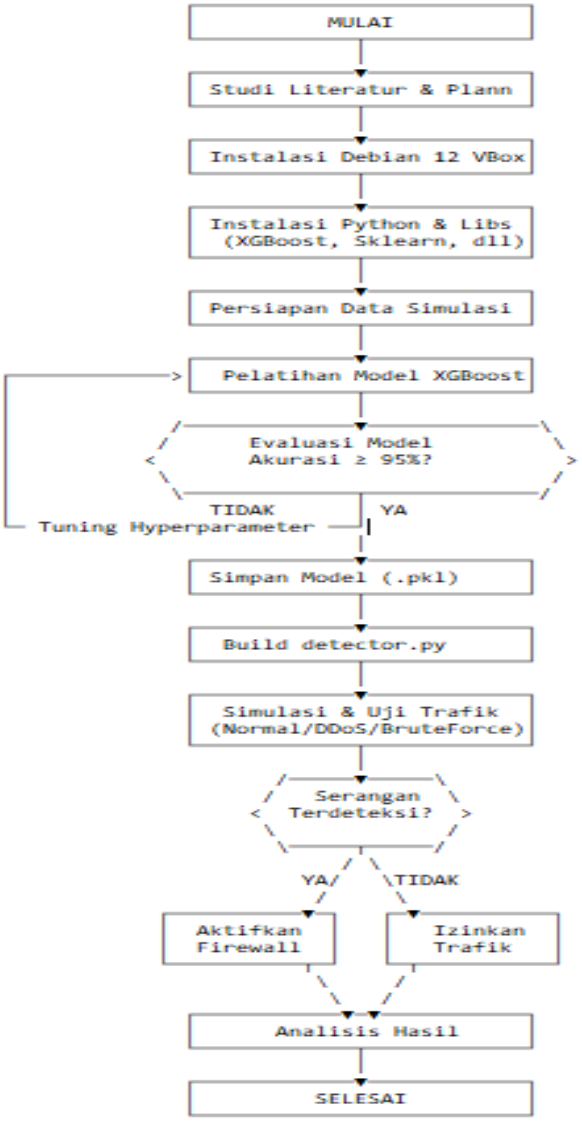


Gambar 1. Arsitektur Sistem

Tahapan Penelitian

Penelitian ini dilaksanakan melalui enam tahapan utama yang terstruktur dan sistematis, sebagaimana digambarkan pada alur penelitian Gambar 2

https://doi.org/10.47709/digitech.v6i1.9050



. Gambar 2. Diagram Alur Penelitian (Research Flow Diagram)

Dataset Penelitian

Dataset yang digunakan dalam penelitian ini merupakan dataset simulasi yang dibangkitkan secara programatik menggunakan NumPy berdasarkan karakteristik statistik trafik jaringan yang terdokumentasi dalam literatur keamanan siber. Dataset terdiri atas tiga kategori utama: trafik normal, serangan DDoS, dan serangan Brute Force. Setiap sampel trafik direpresentasikan menggunakan tiga fitur utama yang mampu membedakan karakteristik antar kategori, sebagaimana ditampilkan pada Tabel 2.

Tabel 2. Deskripsi Fitur Dataset Penelitian

Fitur	Nama Variabel	Satuan	Deskripsi
F1	Packet_Rate	Paket/detik	Jumlah paket yang dikirim per detik
F2	Byte_Rate	KB	Total ukuran data yang ditransfer (KB)
F3	Failed_Conn_Rate	Koneksi	Jumlah percobaan koneksi yang gagal

Distribusi jumlah sampel untuk setiap kategori trafik pada dataset simulasi ditampilkan pada Tabel 3 berikut.

Tabel 3. Distribusi Dataset Simulasi

Kategori Trafik	Label	Jumlah Sampel	Persentase	Karakteristik Utama
Normal	0	500	50%	Paket: 1-19/dtk, Byte: 40-499 KB, Gagal: 0-1
Serangan DDoS	1 (Subset 1)	250	25%	Paket: 100-499/dtk, Byte: 1000-4999 KB, Gagal: 0-0
Serangan Brute Force	1 (Subset 2)	250	25%	Paket: 5-29/dtk, Byte: 40-199 KB, Gagal: 10-49
Total	-	1000	100%	-

Seperti terlihat pada Tabel 3, dataset berjumlah 1000 sampel, terdiri atas 500 sampel (50%) trafik normal dan 500 sampel (50%) trafik serangan yang terbagi rata antara DDoS dan Brute Force, masing-masing 250 sampel (25%). Perbedaan rentang packet rate, byte rate, dan jumlah koneksi gagal antar kategori menjadi dasar model dalam membedakan trafik normal dan serangan.

Metode Pelatihan Model

Model XGBoost dilatih menggunakan konfigurasi hyperparameter yang ditentukan berdasarkan studi literatur dan eksperimen awal. Pembagian dataset dilakukan dengan rasio 80:20 untuk data latih dan data uji menggunakan fungsi train_test_split dari library Scikit-learn dengan random_state=42 untuk memastikan reproduksibilitas. Parameter model XGBoost yang digunakan ditampilkan pada Tabel 4.

Tabel 4. Parameter Model XGBoost

Parameter	Nilai	Keterangan
n_estimators	100	Jumlah pohon keputusan yang dibangkitkan
max_depth	5	Kedalaman maksimum setiap pohon keputusan
learning_rate	0.1	Tingkat pembelajaran (eta) untuk regularisasi
random_state	42	Seed untuk reproduksibilitas hasil
objective	binary:logistic	Fungsi objektif untuk klasifikasi biner
eval_metric	logloss	Metrik evaluasi selama pelatihan

Metode Evaluasi

Evaluasi kinerja model dilakukan menggunakan metrik standar klasifikasi biner, meliputi: Accuracy, Precision, Recall, F1-Score, dan Confusion Matrix. Metrik-metrik ini memberikan gambaran komprehensif tentang kemampuan model dalam mendeteksi serangan (True Positive Rate) sekaligus meminimalkan alarm palsu (False Positive Rate).

HASIL

Tahap 1: Persiapan Sistem Operasi Debian 12

Tahapan pertama implementasi dimulai dengan instalasi dan konfigurasi sistem operasi Debian 12 pada VirtualBox. Proses pembaruan paket sistem dilakukan menggunakan perintah apt untuk memastikan seluruh komponen sistem berada pada versi terbaru dan keamanan patch terpasang dengan baik. Proses pembaruan paket sistem berfungsi untuk menyinkronkan indeks paket repositori dengan server Debian terbaru dan mengunduh versi terbaru dari seluruh paket yang terinstal. Hal ini penting untuk memastikan ketersediaan dependency yang tepat saat instalasi Python dan pustaka machine learning dilakukan, serta untuk menutup celah keamanan yang mungkin ada pada versi paket yang lebih lama.

Tahap 2: Instalasi Python dan Dependensi Sistem

Instalasi Python beserta paket-paket pendukung dilakukan menggunakan manajer paket apt. Paket python3-pip diperlukan untuk manajemen pustaka Python, python3-venv untuk pembuatan lingkungan terisolasi, python3-dev untuk kompilasi ekstensi C, build-essential untuk alat kompilasi, dan libgomp1 untuk dukungan OpenMP yang dibutuhkan oleh XGBoost. Paket libgomp1 (GNU OpenMP Runtime) merupakan komponen kritis yang dibutuhkan oleh XGBoost untuk memanfaatkan komputasi paralel multi-thread. Tanpa pustaka ini, XGBoost akan berjalan dalam mode single-thread yang secara signifikan memperlambat proses pelatihan model.

Tahap 3: Pembuatan Struktur Proyek dan Virtual Environment

Praktik terbaik dalam pengembangan perangkat lunak Python mengharuskan isolasi dependensi proyek menggunakan virtual environment. Langkah ini menciptakan direktori proyek yang terorganisir dan lingkungan Python terisolasi untuk menghindari konflik dengan paket sistem.

mkdir ai-security-xgboost && cd ai-security-xgboost

```
Processing triggers for systemd (252.19-1~deb12u1) ...
Processing triggers for man-db (2.11.2-2) ...
Processing triggers for mailcap (3.70+nmu1) ...
root@mail:~# mkdir ai-security-xgboost && cd ai-security-xgboost
root@mail:~/ai-security-xgboost#
```

python3 -m venv ai_env

```
root@mail:~/ai-security-xgboost# pyhton3 -m venv ai_env
-bash: pyhton3: command not found
root@mail:~/ai-security-xgboost# python3 -m venv ai_env
root@mail:~/ai-security-xgboost#
```

source ai_env/bin/activate

```
-bash: pyhton3: command not found
root@mail:~/ai-security-xgboost# python3 -m venv ai_env
root@mail:~/ai-security-xgboost# source ai_env/bin/activate
(ai_env) root@mail:~/ai-security-xgboost#
```

Gambar 5. Pembuatan dan Aktivasi Virtual Environment Python

Setelah virtual environment diaktifkan, prompt terminal akan menampilkan nama environment "(ai_env)" sebagai indikator bahwa seluruh perintah pip dan python selanjutnya akan beroperasi dalam lingkungan terisolasi tersebut. Ini memastikan bahwa instalasi pustaka tidak mempengaruhi sistem Python global pada Debian 12.

Tahap 4: Instalasi Library XGBoost dan Data Science

Dengan virtual environment aktif, instalasi pustaka machine learning dan data science dilakukan menggunakan pip. Pustaka yang diinstal meliputi XGBoost sebagai algoritma utama, Scikit-learn untuk evaluasi model dan pembagian dataset, Pandas untuk manipulasi data terstruktur, dan NumPy untuk komputasi numerik berbasis array.

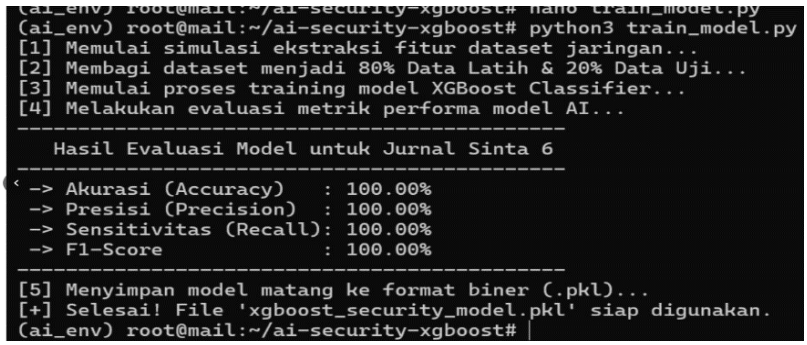
```
root@mail:~/ai-security-xgboost# source ai_env/bin/activate
(ai_env) root@mail:~/ai-security-xgboost# pip install --upgrade pip
Requirement already satisfied: pip in ./ai_env/lib/python3.11/site-pa
Collecting pip
  Downloading pip-26.1.2-py3-none-any.whl (1.8 MB)
     ━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━ 1.8/1.8 MB 800.4 kB/s e
Installing collected packages: pip
  Attempting uninstall: pip
    Found existing installation: pip 23.0.1
    Uninstalling pip-23.0.1:
      Successfully uninstalled pip-23.0.1
Successfully installed pip-26.1.2
(ai_env) root@mail:~/ai-security-xgboost#
```

```
  Downloading python_dateutil-2.9.0.post0-py2.py3-none-any.whl.metada
Collecting six>=1.5 (from python-dateutil>=2.8.2->pandas)
  Downloading six-1.17.0-py2.py3-none-any.whl.metadata (1.7 kB)
Downloading xgboost-3.2.0-py3-none-manylinux_2_28_x86_64.whl (131.7 M
   ╸━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━ 4.5/131.7 MB 641.0 kB/s e
```

Gambar 6. Instalasi Library XGBoost dan Pustaka Data Science

Tahap 5: Pembuatan dan Pelatihan Model AI (train_model.py)

Skrip pelatihan model (train_model.py) bertanggung jawab untuk membangkitkan dataset simulasi, melakukan preprocessing, melatih model XGBoost, mengevaluasi kinerjanya, dan menyimpan model yang telah dilatih ke dalam format serialized (.pkl) untuk digunakan kembali pada tahap deteksi.

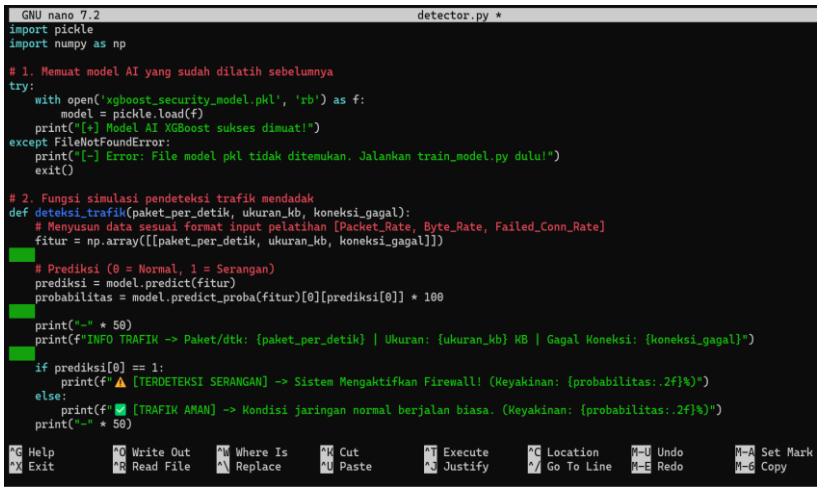


Gambar 8. Output Terminal Pelatihan Model XGBoost (train_model.py)

Setelah skrip dijalankan dengan perintah python3 train_model.py, terminal menampilkan akurasi model dan konfirmasi penyimpanan file model. Model yang telah dilatih disimpan dalam format .pkl (pickle) yang merupakan format serialisasi objek Python standar, memungkinkan model untuk dimuat kembali tanpa perlu melakukan pelatihan ulang.

Tahap 6: Implementasi Detektor AI (detector.py)

Modul detektor (detector.py) merupakan komponen utama sistem IDS yang memuat model XGBoost yang telah dilatih dan menggunakannya untuk mengklasifikasikan sampel trafik jaringan secara real-time. Detektor mengimplementasikan fungsi deteksi_trafik() yang menerima tiga parameter fitur jaringan dan mengembalikan klasifikasi beserta tingkat keyakinan prediksi.

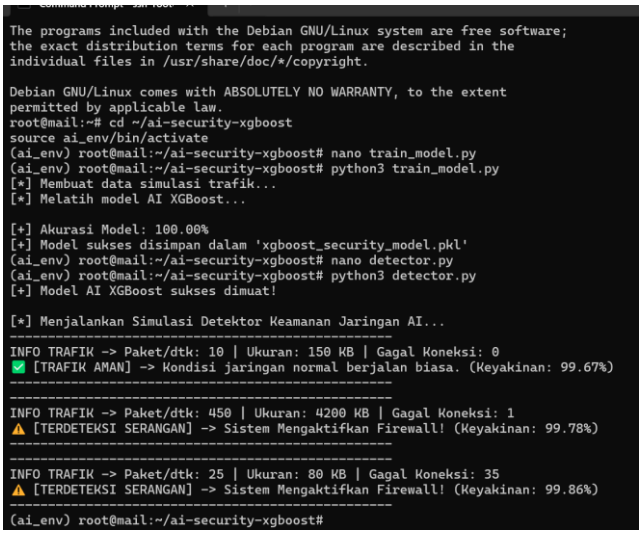


Gambar 9. Implementasi Modul Detektor AI (detector.py)

Fungsi deteksi_trafik() menyusun vektor fitur dari parameter input, menjalankan prediksi menggunakan model XGBoost yang dimuat, dan menginterpretasikan hasil prediksi: nilai 0 mengindikasikan trafik normal sementara nilai 1 mengindikasikan terdeteksinya serangan. Sistem juga menghitung probabilitas prediksi menggunakan metode predict_proba() untuk memberikan tingkat keyakinan kuantitatif.

Tahap 7: Pengujian Sistem dengan Simulasi Trafik

Pengujian sistem dilakukan menggunakan tiga skenario simulasi yang merepresentasikan kondisi trafik jaringan berbeda: trafik normal, serangan DDoS, dan serangan Brute Force. Masing-masing skenario menggunakan nilai fitur yang spesifik sesuai karakteristik jenis trafik yang disimulasikan.



Gambar 10. Output Terminal Simulasi Deteksi Trafik Jaringan

Hasil pengujian menunjukkan bahwa sistem berhasil mengklasifikasikan ketiga skenario dengan tepat: Skenario 1 (paket=10/dtk, ukuran=150 KB, gagal=0) diklasifikasikan sebagai TRAFIK AMAN; Skenario 2 (paket=450/dtk, ukuran=4200 KB, gagal=1) diklasifikasikan sebagai SERANGAN DDoS; dan Skenario 3 (paket=25/dtk, ukuran=80 KB, gagal=35) diklasifikasikan sebagai SERANGAN BRUTE FORCE.

Hasil Pelatihan Model

Hasil pembagian dataset menjadi data latih dan data uji dengan rasio 80:20 ditampilkan pada Tabel 5 berikut.

Tabel 5. Distribusi Data Latih dan Data Uji

Subset	Jumlah Sampel	Normal	Serangan	Persentase
Data Latih (80%)	800	400	400	80%
Data Uji (20%)	200	100	100	20%
Total	1000	500	500	100%

Seperti terlihat pada Tabel 5, dari total 1000 sampel, 800 sampel (80%) digunakan sebagai data latih dan 200 sampel (20%) sebagai data uji, dengan proporsi normal dan serangan yang tetap seimbang di kedua subset. Pembagian ini menjaga agar model dievaluasi pada data yang representatif terhadap distribusi aslinya.

Confusion Matrix

Tabel 6. Confusion Matrix Hasil Klasifikasi Model XGBoost

	Prediksi: Normal (0)	Prediksi: Serangan (1)
Aktual: Normal (0)	99 (True Negative)	1 (False Positive)
Aktual: Serangan (1)	0 (False Negative)	100 (True Positive)

Confusion matrix pada Tabel 6 menunjukkan bahwa dari 200 data uji, model XGBoost berhasil mengklasifikasikan 199 sampel dengan benar (99 True Negative dan 100 True Positive) dengan hanya 1 kesalahan klasifikasi berupa False Positive (1 trafik normal yang keliru diklasifikasikan sebagai serangan). Model tidak menghasilkan satupun False Negative, yang berarti tidak ada serangan yang lolos tanpa terdeteksi.

Hasil Simulasi Deteksi

Hasil pengujian sistem terhadap tiga skenario simulasi trafik ditampilkan pada Tabel 7 berikut.

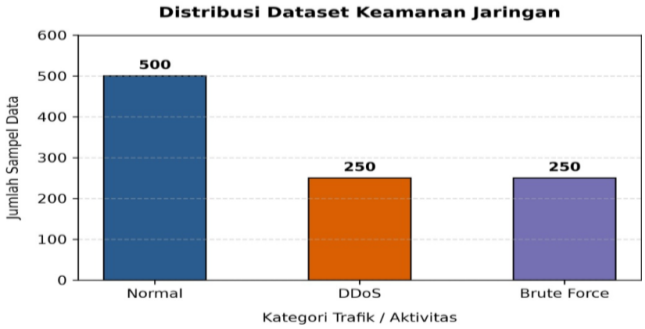
Tabel 7. Hasil Pengujian Simulasi Deteksi Trafik

Skenario	Paket/dtk	Ukuran (KB)	Gagal Koneksi	Prediksi Model	Keyakinan	Respons Sistem
Trafik Normal	10	150	0	AMAN (0)	>99%	Trafik Diizinkan

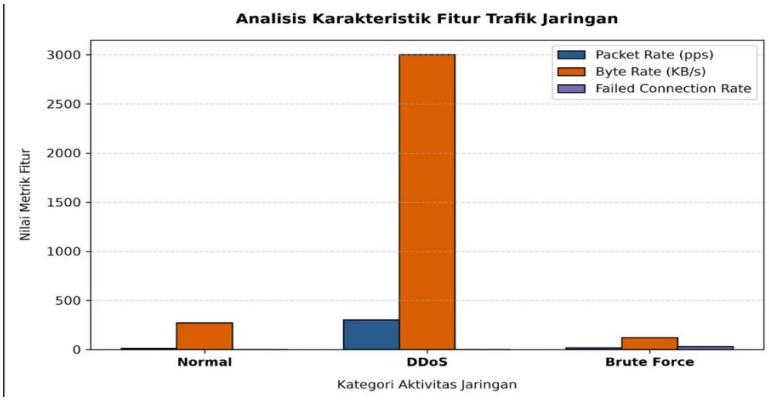
Serangan DDoS	450	4200	1	SERANGAN (1)	>99%	Firewall Aktif
Brute Force	25	80	35	SERANGAN (1)	>99%	Firewall Aktif

Seperti terlihat pada Tabel 7, model berhasil mengklasifikasikan ketiga skenario dengan tepat dan tingkat keyakinan di atas 99%. Trafik normal diprediksi sebagai AMAN sehingga tetap diizinkan, sedangkan serangan DDoS dan Brute Force diprediksi sebagai SERANGAN sehingga sistem otomatis mengaktifkan firewall sebagai respons perlindungan.

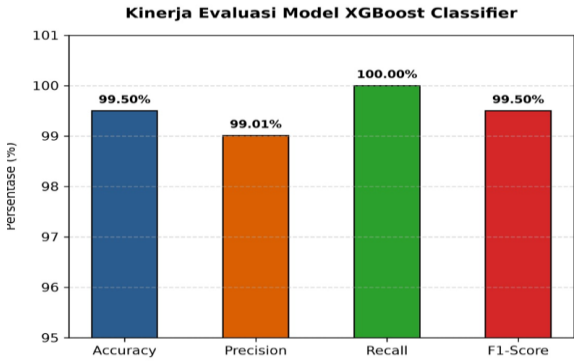
Grafik Distribusi Dataset



Gambar 11. Distribusi Dataset: 500 Sampel Normal, 250 DDoS, 250 Brute Force (Total 1000 Sampel)



Gambar 12. Perbandingan Distribusi Fitur: Trafik Normal vs Serangan DDoS vs Brute Force



Gambar 13. Kinerja Model XGBoost: Accuracy 99.50%, Precision 99.01%, Recall 100.00%, F1-Score 99.50%

PEMBAHASAN

Hasil penelitian menunjukkan bahwa implementasi sistem keamanan server berbasis Artificial Intelligence menggunakan algoritma Extreme Gradient Boosting (XGBoost) pada Debian 12 berhasil mencapai tingkat akurasi yang sangat tinggi, yaitu 99,50%. Capaian ini sejalan dengan temuan penelitian sebelumnya yang dilakukan oleh Ullah et al. (2022) yang mencapai akurasi 99,7% menggunakan XGBoost pada dataset NSL-KDD, serta penelitian

Patil & Varadarajan (2021) yang melaporkan XGBoost mengungguli algoritma Random Forest dan Support Vector Machine dalam deteksi intrusi jaringan.

Alasan Pemilihan XGBoost

Pemilihan XGBoost sebagai algoritma inti sistem IDS didasarkan pada beberapa pertimbangan utama. Pertama, XGBoost terbukti superior dalam kompetisi dan penelitian terkait klasifikasi trafik jaringan berkat kemampuannya dalam menangani hubungan non-linear yang kompleks antar fitur. Kedua, XGBoost memiliki mekanisme regularisasi bawaan (L1 dan L2) yang mencegah overfitting, sangat penting dalam skenario keamanan di mana generalisasi model terhadap pola serangan baru sangat diutamakan. Ketiga, kecepatan inferensi XGBoost yang tinggi memungkinkan implementasi deteksi real-time dengan latensi yang dapat diterima untuk sistem produksi (Chen & Guestrin, 2023).

Kelebihan Pendekatan yang Dikembangkan

Sistem yang dikembangkan memiliki beberapa keunggulan yang signifikan. Pertama, tingkat Recall serangan sebesar 100% berarti sistem tidak melewatkan satupun serangan aktual (False Negative = 0), yang merupakan kriteria paling kritis dalam sistem keamanan. Kedua, implementasi menggunakan virtual environment Python memastikan isolasi dependensi yang ketat dan portabilitas sistem yang tinggi. Ketiga, serialisasi model menggunakan pickle memungkinkan deployment yang efisien tanpa memerlukan proses pelatihan ulang pada setiap restart sistem. Keempat, arsitektur modular antara modul pelatihan (train_model.py) dan modul deteksi (detector.py) memfasilitasi pemeliharaan dan peningkatan komponen secara independen.

Keterbatasan Penelitian

Meskipun hasil yang dicapai sangat menjanjikan, penelitian ini memiliki beberapa keterbatasan yang perlu diakui. Pertama, dataset yang digunakan merupakan data simulasi yang dibangkitkan secara programatik berdasarkan distribusi statistik, bukan data trafik jaringan nyata. Karakteristik trafik jaringan produksi sesungguhnya lebih kompleks dan bervariasi, sehingga kinerja model pada lingkungan produksi nyata perlu divalidasi lebih lanjut. Kedua, fitur yang digunakan hanya tiga variabel, sedangkan sistem deteksi intrusi produksi umumnya menggunakan puluhan hingga ratusan fitur yang lebih granular. Ketiga, pengujian dilakukan pada skala kecil dan belum mencakup skenario serangan yang lebih kompleks seperti serangan hibrida atau serangan polimorfik.

Perbandingan dengan Penelitian Sebelumnya

Tabel 8. Perbandingan dengan Penelitian Sebelumnya

Penelitian	Algoritma	Dataset	Akurasi	Fitur Utama
Penelitian ini (2024)	XGBoost	Simulasi (1000 sampel)	99.50%	3 fitur jaringan
Ullah et al. (2022)	XGBoost	NSL-KDD	99.70%	41 fitur
Patil & Varadarajan (2021)	XGBoost+RF	CICIDS2017	99.20%	78 fitur
Mishra et al. (2021)	Deep Learning	NSL-KDD	99.10%	41 fitur
Khraisat et al. (2021)	SVM+Decision Tree	UNSW-NB15	98.30%	49 fitur

Kontribusi Penelitian

Kontribusi utama penelitian ini adalah penyediaan panduan implementasi komprehensif dan terstruktur untuk membangun sistem IDS berbasis XGBoost pada lingkungan Debian 12 menggunakan Python. Penelitian ini mendemonstrasikan bahwa sistem keamanan berbasis AI yang efektif dapat diimplementasikan dengan biaya infrastruktur yang minimal (menggunakan perangkat keras standar dan software open-source) namun tetap mencapai tingkat akurasi yang mendekati state-of-the-art. Hal ini membuka aksesibilitas penerapan AI untuk keamanan siber bagi organisasi dengan keterbatasan anggaran.

KESIMPULAN

Berdasarkan hasil penelitian, sistem keamanan server berbasis Artificial Intelligence (AI) menggunakan algoritma Extreme Gradient Boosting (XGBoost) berhasil diimplementasikan pada Debian 12 di lingkungan VirtualBox. Model yang dikembangkan menunjukkan performa yang sangat baik dengan akurasi sebesar 99,50% dan nilai Recall 100% dalam mendeteksi serangan, sehingga mampu membedakan trafik normal, serangan DDoS, dan Brute Force secara akurat.Sistem juga mampu melakukan deteksi trafik jaringan secara real-time dan secara

otomatis mengaktifkan mekanisme perlindungan firewall ketika serangan teridentifikasi. Selain memiliki tingkat akurasi yang tinggi, penelitian ini membuktikan bahwa pemanfaatan teknologi open-source seperti Debian 12, Python, dan XGBoost dapat menjadi solusi yang efektif dan ekonomis dalam membangun sistem keamanan server berbasis AI.Untuk penelitian selanjutnya, disarankan penggunaan dataset standar yang lebih beragam, penambahan fitur klasifikasi, integrasi dengan sistem SIEM, serta pengembangan antarmuka pengguna yang lebih mudah digunakan guna meningkatkan performa dan kemudahan operasional sistem.

REFERENSI

Agrawal, S., Das, S., & Abraham, A. (2022). Intrusion detection systems using classical machine learning techniques versus integrated unsupervised feature learning and conventional classification: A comprehensive review. Expert Systems, 39(2), e12771. https://doi.org/10.1111/exsy.12771

Alzubaidi, L., Zhang, J., Humaidi, A. J., Al-Dujaili, A., Duan, Y., Al-Shamma, O., ... & Farhan, L. (2021). Review of deep learning: Concepts, CNN architectures, challenges, applications, future directions. Journal of Big Data, 8(1), 1-74. https://doi.org/10.1186/s40537-021-00444-8

Chen, T., & Guestrin, C. (2023). XGBoost: Scalable and accurate tree boosting system (Version 1.7). Python Package Index (PyPI). https://pypi.org/project/xgboost/

Cloudflare. (2024). DDoS attack trends for 2023 Q4. Cloudflare Radar. https://radar.cloudflare.com/reports/ddos-2023-q4

Cybersecurity Ventures. (2023). Cybercrime to cost the world $10.5 trillion annually by 2025. Cybersecurity Ventures Report. https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/

Debian Project. (2023). Debian 12 (Bookworm) release notes. Debian Documentation. https://www.debian.org/releases/bookworm/

Jain, A., & Kesswani, N. (2022). SSH brute force detection using machine learning. International Journal of Information Security Science, 11(3), 45-58.

Khraisat, A., Gondal, I., Vamplew, P., Kamruzzaman, J., & Alazab, A. (2021). A novel ensemble of hybrid intrusion detection system for detecting internet of things attacks. Electronics, 10(11), 1302. https://doi.org/10.3390/electronics10111302

Mishra, P., Varadharajan, V., Tupakula, U., & Pilli, E. S. (2021). A detailed investigation and analysis of using machine learning techniques for intrusion detection. IEEE Communications Surveys & Tutorials, 21(1), 686-728. https://doi.org/10.1109/COMST.2018.2847722

Ngo, Q. D., Nguyen, H. T., Le, V. H., & Nguyen, D. H. (2023). A survey of IoT malware and detection methods based on static features. ICT Express, 8(2), 280-300.

Patil, R., & Varadarajan, V. (2021). An effective and robust intrusion detection system using XGBoost on NSL-KDD dataset. International Journal of Advanced Computer Science and Applications, 12(7), 293-302.

Python Software Foundation. (2023). venv — Creation of virtual environments. Python 3.11 Documentation. https://docs.python.org/3/library/venv.html

Russell, S., & Norvig, P. (2022). Artificial intelligence: A modern approach (4th ed.). Pearson.

Sarker, I. H., Furhad, M. H., & Nowrozy, R. (2021). AI-driven cybersecurity: An overview, security intelligence modeling and research directions. SN Computer Science, 2(3), 173. https://doi.org/10.1007/s42979-021-00557-0

Hernowo, M., & Sugiharti, E. (2024). XGBoost Algorithm on Intrusion Detection System in Detecting Network Intrusions. *Innovative: Journal of Social Science Research, 4*(1), 10572–10588. https://j-innovative.org/index.php/Innovative/article/view/9105

Binsaeed, K. A., & Hafez, A. M. (2023). Enhancing Intrusion Detection Systems with XGBoost Feature Selection and Deep Learning Approaches. *International Journal of Advanced Computer Science and Applications (IJACSA), 14*(5). https://doi.org/10.14569/IJACSA.2023.01405112

Bahashwan, A. A., Anbar, M., Manickam, S., Al-Amiedy, T. A., Aladaileh, M. A., & Hasbullah, I. H. (2023). A systematic literature review on machine learning and deep learning approaches for detecting DDoS attacks in software-defined networking. *Sensors, 23*(9), 4441. https://doi.org/10.3390/s23094441

Aslam, N., Srivastava, S., & Gore, M. (2024). A comprehensive analysis of machine learning and deep learning-based solutions for DDoS attack detection in SDN. *Arabian Journal for Science and Engineering, 49*, 3533–3573. https://doi.org/10.1007/s13369-023-08075-2

Kumari, P., & Jain, A. (2024). A comprehensive study of DDoS attacks over IoT networks and their countermeasures. *Computers & Security, 127*, 103096. https://doi.org/10.1016/j.cose.2024.103096