Penggunaan Random Forest dan Analisis Perilaku untuk Prediksi Serangan DDoS dalam Lingkungan Cloud Computing

Use of Random Forest and Behavioral Analysis for DDoS Attack Prediction in Cloud Computing Environments

Andi Prayogi*[1], Muhammad Akbar Syahbana Pane[2], Rahmad Dian[2], Ratu Mutiara Siregar[2], Raden Aris Sugianto[2], Hasanal Fachri Satia Simbolon[2]
[1,2] Sistem dan Teknologi Informasi, Institut Teknologi Sawit Indonesia, Indonesia
E-mail: [1*]andiprayogi@itsi.ac.id
*: Penulis korenspondensi (corresponding author)

Abstrak

Dalam dunia komputasi awan yang semakin berkembang, ancaman serangan Distributed Denial of Service (DDoS) menjadi isu yang sangat krusial. Penelitian ini bertujuan untuk mengembangkan dan mengimplementasikan model prediksi serangan DDoS menggunakan algoritma Random Forest dan analisis perilaku jaringan. Dataset CICIDS2017 digunakan sebagai sumber data utama untuk melatih dan menguji model prediksi yang dikembangkan. Pemilihan algoritma Random Forest didasarkan pada kemampuannya yang tinggi dalam menangani data besar dan kompleks serta kemampuannya dalam mengenali pola anomali yang sering menjadi indikasi serangan siber. Hasil pengujian menunjukkan bahwa model ini mencapai akurasi yang signifikan dengan precision sebesar 97,8%, recall sebesar 98,2%, dan F1-score sebesar 98,0%. Analisis perilaku jaringan yang diterapkan, melibatkan fitur-fitur dinamis seperti waktu antar paket (Inter-Arrival Time/IAT), ukuran rata-rata segmen, dan jumlah paket per detik, yang terbukti efektif dalam meningkatkan kemampuan deteksi model. Implementasi model dalam lingkungan komputasi awan menunjukkan bahwa metode ini dapat diintegrasikan dengan sistem deteksi intrusi (Intrusion Detection Systems/IDS) yang sudah ada untuk memberikan lapisan perlindungan tambahan terhadap serangan DDoS. Berdasarkan hasil yang diperoleh, penelitian ini merekomendasikan penggunaan kombinasi algoritma Random Forest dan analisis perilaku jaringan sebagai solusi yang efektif untuk mendeteksi serangan DDoS dalam lingkungan komputasi awan. Penelitian lanjutan disarankan untuk mengembangkan dan menguji model dengan dataset yang lebih beragam serta mengoptimalkan algoritma untuk meningkatkan performa deteksi.

Kata kunci: Random Forest, DDoS, Cloud Computing

Abstract

In the ever-evolving world of cloud computing, the threat of Distributed Denial of Service (DDoS) attacks has become a critical issue. This study aims to develop and implement a DDoS attack prediction model using the Random Forest algorithm and network behavior analysis. The CICIDS2017 dataset was utilized as the primary data source for training and testing the developed prediction model. The selection of the Random Forest algorithm is based on its high capability in handling large and complex datasets, as well as its proficiency in recognizing anomalous patterns indicative of cyber attacks. Testing results indicate that the model achieved significant accuracy with a precision of 97.8%, recall of 98.2%, and F1-score of 98.0%. The applied network behavior analysis involved dynamic features such as Inter-Arrival Time (IAT), average segment size, and packets per second, which proved effective in enhancing the model's detection capabilities. Implementation of the model in a cloud computing environment demonstrated that this method could be integrated with existing Intrusion Detection Systems (IDS) to provide an additional layer of protection against DDoS attacks. Based on the obtained results, this study recommends the use of a combination of the Random Forest algorithm and

network behavior analysis as an effective solution for detecting DDoS attacks in cloud computing environments. Further research is suggested to develop and test the model with more diverse datasets and to optimize the algorithm for improved detection performance.

Keywords: Random Forest. DDoS, Cloud Computing

1. PENDAHULUAN

Teknologi Cloud Computing, atau Teknologi Komputasi Awan, memungkinkan penyimpanan data secara maya di server yang dapat diakses melalui jaringan internet[1]. Komputasi awan membuat akses pengguna melalui jarak jauh atau biasa dikenal dengan akses control melalui sebuah remote menggunakan port protocol remote seperti SSH (Secure Shell) nomor port 22 dan sebagainya[2]. Aksesibilitasnya dipengaruhi oleh kestabilan jaringan yang digunakan penggunanya.

Meskipun teknologi ini menawarkan kemudahan akses dan fleksibilitas, hal ini juga memperkenalkan tantangan baru dalam hal keamanan, terutama terkait dengan serangan Distributed Denial of Service (DDoS) [3]. Serangan DDoS, di mana penyerang menggunakan berbagai sistem terdistribusi untuk membanjiri target dengan lalu lintas yang sangat besar[4].

Distributed Denial of Service (DDoS) adalah jenis serangan siber di mana penyerang menggunakan beberapa sistem terdistribusi untuk mengirim sejumlah besar permintaan atau lalu lintas ke target tertentu, seperti server, jaringan, atau layanan online[5]. Tujuan utama dari serangan ini adalah untuk membuat layanan target menjadi tidak tersedia bagi pengguna sah dengan membanjiri sistem dengan lalu lintas yang luar biasa besar sehingga sistem tidak dapat menangani permintaan yang sah[6].

Dalam beberapa tahun terakhir, serangan DDoS di Indonesia menunjukkan tren yang mengkhawatirkan, dengan kerugian ekonomi yang meningkat dari tahun ke tahun[7]. Beberapa serangan online dapat diatasi melalui keamanan siber. Infrastruktur cloud yang dinamis dan tersebar secara geografis membutuhkan pendekatan keamanan yang lebih canggih[8]. Berbagai macam jenis keamanan siber dan beberapa metode yang diterapkan berhasil mengamankan koneksi jaringan yang terhubung pada komputasi awan[9]. Meskipun berbagai teknik keamanan telah diterapkan untuk melindungi infrastruktur cloud, teknik tradisional sering kali tidak memadai untuk menangani volume data yang besar dan kompleksitas serangan yang semakin berkembang [10].

Teknik tradisional seperti Threshold-Based Detection, meskipun sederhana, seringkali rentan terhadap alarm palsu dan tidak dapat menangani lonjakan lalu lintas yang sah [11]. Teknik ini menetapkan ambang batas tertentu pada parameter lalu lintas jaringan seperti jumlah paket perdetik atau total volume data. Jika lalu lintas melebihi batas yang ditentukan sistem akan menganggapnya sebagai serangan. Teknik tersebut masih memiliki kelemahan seperti rentan terhadap alarm palsu ketika ada lonjakan lalu lintas yang sah[12].

Untuk mengatasi keterbatasan teknik tradisional, pendekatan modern menggunakan machine learning telah diperkenalkan[13]. Algoritma machine learning, seperti Random Forest, menawarkan keunggulan dalam mendeteksi ancaman dengan mengurangi kelemahan sistem lama [14].

Algoritma Random Forest merupakan salah satu teknik pembelajaran mesin yang telah terbukti efektif dalam berbagai aplikasi, termasuk deteksi ancaman siber. Algoritma ini bekerja dengan membangun sejumlah besar pohon keputusan selama pelatihan dan menggabungkan prediksi dari masing-masing pohon untuk menentukan hasil akhir[15]. Random Forest, sebagai metode ensemble learning yang membangun banyak pohon keputusan, terbukti efektif dalam berbagai aplikasi termasuk deteksi ancaman siber[16]. Algoritma machine learning, seperti Random Forest, menawarkan keunggulan dalam mendeteksi ancaman dengan mengurangi kelemahan sistem lama[17].

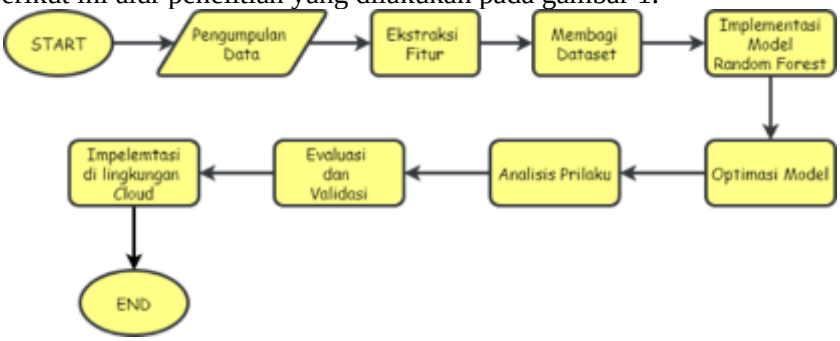
Meskipun banyak penelitian tentang deteksi serangan DDoS dan penggunaan machine learning, ada kekurangan dalam penerapan spesifik algoritma Random Forest dalam lingkungan

cloud computing. Penelitian yang ada sering kali tidak membahas bagaimana algoritma ini dapat diterapkan dalam konteks cloud dan menguji efektivitasnya menggunakan metodologi pengujian yang inovatif.

Berdasarkan ulasan literatur dan identifikasi research gap, penelitian ini bertujuan untuk mengeksplorasi penerapan algoritma Random Forest dalam deteksi serangan DDoS di lingkungan cloud computing. Penelitian ini akan mengisi kekurangan dalam literatur dengan mengadaptasi Random Forest untuk keamanan siber di cloud, menggunakan dataset CICIDS2017, dan mengembangkan metodologi pengujian menggunakan aplikasi "POSTMAN" untuk mensimulasikan serangan DDoS. Dengan demikian, penelitian ini diharapkan dapat memberikan kontribusi signifikan dalam memperluas pengetahuan tentang deteksi DDoS dalam konteks cloud computing.

2. METODE PENELITIAN

Penelitian ini berfokus pada penerapan algoritma Random Forest dan analisis perilaku untuk mendeteksi serangan Distributed Denial of Service (DDoS) dalam lingkungan cloud computing. Metode penelitian ini dirancang untuk memastikan pendekatan yang komprehensif dan sistematis dalam mengidentifikasi, menganalisis, dan mengevaluasi efektivitas teknik yang diusulkan. Berikut ini alur penelitian yang dilakukan pada gambar 1.



Gambar 1. Alur Penelitian Analisis Prilaku Serangan DDoS dan Algoritma Random Forest

2.1 Pengumpulan Data

Pengumpulan data dilakukan untuk menguji algoritma dan jenis-jenis serangan yang dilakukan. Sumber data yang dipakai menggunakan dataset publik CICIDS2017 yang disediakan oleh Canadian Institute For Cybersecurity. Dataset ini mencakup berbagai jenis serangan termasuk DDoS dan dirancang untuk memberikan data lalu lintas jaringan yang realistis untuk keamanan siber.

Setelah dataset terkumpul selanjutnya melakukan pembersihan data dengan menghilangkan noise dan mengisi nilai yang hilang dalam dataset dan melakukan normalisasi fitur untuk memastikan skala yang konsisten diseluruh dataset. Tahapan proses ini seluruhnya menggukana bahasa Program Python dengen format dataset Json.

Dataset CICIDS2017 berisi data lalu lintas jaringan yang mencakup beberapa jenis serangan siber seperti DDoS, brute force, dan rekayasa sosial. Dataset ini dibagi menjadi beberapa bagian berdasarkan skenario serangan yang berbeda. Contoh fitur yang ada pada tabel 1 dataset ini adalah:

Tabel 1 Isi Kriteria Dataset CICIDS2017

Nama Kriteria	Keterangan
Complete Network Configuration	Topologi jaringan lengkap mencakup Modem, Firewall, Switch, Router, dan kehadiran berbagai sistem operasi seperti Windows, Ubuntu, dan Mac OS X

Complete Traffic	Dengan memiliki agen profil pengguna dan 12 mesin berbeda di Jaringan Korban dan serangan nyata dari Jaringan Serangan
Labelled Dataset	menunjukkan label jinak dan serangan untuk setiap hari. Selain itu, rincian waktu serangan akan dipublikasikan pada dokumen kumpulan data.
Complete Interaction	Antara LAN internal dengan memiliki dua jaringan berbeda dan juga komunikasi Internet
Complete Capture	menggunakan port cermin, seperti sistem penyadapan, semua lalu lintas telah ditangkap dan dicatat di server penyimpanan
Available Protocols	Menyediakan keberadaan semua protokol umum yang tersedia, seperti protokol HTTP, HTTPS, FTP, SSH, dan email
Attack Diversity	Termasuk serangan paling umum berdasarkan laporan McAfee 2016, seperti berbasis Web, Brute force, DoS, DDoS, Infiltrasi, Heart-bleed, Bot, dan Scan yang tercakup dalam kumpulan data ini
Heterogeneity	Menangkap lalu lintas jaringan dari Switch utama dan dump memori serta panggilan sistem dari semua mesin korban, selama eksekusi serangan.
Feature Set	Mengekstraksi lebih dari 80 fitur aliran jaringan dari lalu lintas jaringan yang dihasilkan menggunakan CICFlowMeter dan mengirimkan kumpulan data aliran jaringan sebagai file CSV. Lihat penganalisis PCAP dan generator CSV
Metadata	Menjelaskan secara lengkap dataset yang meliputi waktu, serangan, alur dan label pada makalah yang diterbitkan

2.2 Ekstraksi Fitur

Ekstraksi fitur adalah langkah penting dalam mempersiapkan dataset untuk pelatihan model pembelajaran mesin. Pada penelitian ini, fitur-fitur yang diekstraksi dari dataset CICIDS2017 akan digunakan untuk melatih model Random Forest dalam mendeteksi serangan DDoS. Berikut adalah Langkah-langkah dan rumus yang digunakan dalam ekstraksi fitur:

Langkah-Langkah Ekstraksi Fitur

Tahap 1 Identifikasi Fitur Penting

Identifikasi fitur yang terdapat di dalam dataset. Fitur tersebut adalah ada pada gambar 1

Tahap 2 Transformasi Fitur

Tranformasi fitur menggunakan metode normalisasi data dan reduksi dimensi. Normalisasi data menggunakan teknik standarisasi untuk memastikan bahwa semua fitur berada dalam skala yang sama. Berikut adalah rumus normalisasi menggunakan Z-score:

$$z = \frac{(X-\mu)}{\sigma} \qquad (1)$$

Dimana:

X = adalah nilai fitur

μ = adalah rata-rata

σ = adalah standar deviasi dari fitur tersebut

Reduksi Dimensi menggunakan Principal Component Analysis (PCA) untuk mengurangi dimensi data tanpa kehilangan informasi penting. Berikut adalah prosesnya:

1. Standarisasi data, mengubah data ke skala yang sama.
2. Matriks Kovarians:
   Menghitung Matriks Kovarian untuk data
   $\sum = \frac{1}{n-1}(X^T X)$ (2)
3. Eigenvalue dan Eigenvector:
   Menghitung eigenvalue dan eigenvector dari matriks kovarians
4. Proyek Data
   Memproyeksikan data ke ruang dimensi yang lebih rendah menggunakan eigenvector utama.

2.3 Pembagian Dataset

Membagi dataset menjadi data latih (training) dan data uji (testing) dengan proporsi 70:30 untuk memastikan model dapat dievaluasi secara objektif.

2.4 Implementasi Model Random Forest

Implementasi model Random Forest adalah salah satu langkah kunci dalam penelitian ini untuk mendeteksi serangan DDoS. Berikut adalah rincian langkah-langkah, rumus yang digunakan, dan alur implementasi model Random Forest secara detail.

Langkah-langkah Implementasi model Random Forest

1. Inisialisasi Model
   - Tentukan parameter awal seperti jumlah pohon (n_estimators) dan kedalaman maksimum pohon (max_depth).
   - Parameter yang digunakan Parameter: n_estimators = 100, max_depth = 20, random_state = 42.
2. Pelatihan Model
   Latih model menggunakan data latih yang telah dipersiapkan sebelumnya.
3. Evaluasi Awal
   Gunakan data uji untuk mengevaluasi performa awal model dengan metrik seperti akurasi, precision, recall, dan F1-score.
4. Optimasi Model
   - Gunakan GridSearchCV untuk menemukan kombinasi parameter terbaik: n_estimators = [100, 200, 300], max_depth = [10, 20, 30].
   - Latih ulang model dengan parameter yang optimal.
5. Validasi dan Analisis Hasil
   Lakukan validasi silang dan analisis hasil menggunakan berbagai metrik evaluasi.

Setiap pohon dalam Random Forest adalah pohon keputusan yang dibangun dengan memecah dataset berdasarkan fitur yang memaksimalkan pengurangan impuritas. Impuritas dihitung menggunakan Gini Impurity atau Entropy.

Gini Impurity:

$$Gini(D) = 1 - \sum_{i=1}^{C} p_i^2 \quad (3)$$

Di mana pi adalah proporsi sampel yang termasuk dalam kelas i dan C adalah jumlah kelas.

Entropy:

$$Entropy(D) = -\sum_{i=1}^{C} p_i log_2(p_i) \quad (4)$$

Random Forest:
Algoritma Random Forest membangun sejumlah pohon keputusan (n) dan menggabungkan prediksi dari setiap pohon untuk menentukan hasil akhir menggunakan voting mayoritas.

$$y_{final} = mode\{y1, y2, y3 \dots, yn\} \quad (5)$$

Di mana $y1$,$y2$,...,yn adalah prediksi dari masing-masing pohon.

2.5 Evaluasi dan Validasi

Menggunakan metrik evaluasi seperti akurasi, precision, recall, dan F1-score untuk menilai performa model yang dioptimalkan. Melakukan validasi silang (cross-validation) untuk memastikan keandalan model. Membandingkan hasil deteksi serangan DDos dengan teknik tradisional untuk menunjukkan keunggulan pendekatan yang diusulkan.

2.6 Implementasi di Lingkungan Cloud

Mengintegrasikan model yang telah dilatih dan dioptimalkan ke dalam sistem cloud computing untuk deteksi real-time. Menggunakan layanan cloud seperti AWS, Google Cloud, atau Azure untuk mengimplementasikan dan menguji model. Memantau performa model dan respon terhadap serangan DDoS secara real-time. Mengimplementasikan mekanisme mitigasi untuk mengurangi dampak serangan berdasarkan deteksi model.

3. HASIL DAN PEMBAHASAN

Penelitian ini menggunakan model Random Forest untuk mendeteksi serangan Distributed Denial of Service (DDoS) dalam lingkungan Cloud Computing, menggunakan dataset CICIDS2017. Hasil penelitian yang diperoleh melalui beberapa tahap yang sistematis, mulai dari pembacaan dataset, pra-pemrosesan, pelatihan model, hingga evaluasi hasil.

3.1 Pembacaan dan Pengolahan Dataset

Langkah pertama adalah membaca data dari folder yang berisi file CSV dan file CSV yang akan digunakan adalah file CSV yang berisi informasi pada serangan DDoS. File tersebut bernama “Friday-WorkingHours-Afternoon-DDos.pcap_ISC X.csv”

```python
import pandas as pd

# Path ke file CSV
file_path = 'path_to_your_csv_file/Friday-WorkingHours-Afternoon-DDos.pcap_ISCX.csv'

# Membaca data CSV
df = pd.read_csv(file_path)

# Menampilkan beberapa baris pertama dari dataset
print(df.head())

# Tampilkan nama-nama kolom untuk memverifikasi keberadaan kolom 'Label'
print(df.columns)
```

Gambar 2 Pembacaan Dataset CSV ke dalam program

3.2 Optimasi Model dan Algoritma Random Forest

Gunakan GridSearchCV untuk menemukan parameter terbaik, kemudian latih ulang model dengan parameter optimal.

```python
from sklearn.ensemble import RandomForestClassifier
from sklearn.metrics import classification_report, accuracy_score

# Inisialisasi model Random Forest
rf_model = RandomForestClassifier(
    n_estimators=100,
    max_depth=20,
    random_state=42
    )

# Melatih model
rf_model.fit(X_train, y_train)

# Prediksi pada data uji
y_pred = rf_model.predict(X_test)

# Evaluasi model
accuracy = accuracy_score(y_test, y_pred)
report = classification_report(y_test, y_pred)

print("Accuracy:", accuracy)
print("Classification Report:")
print(report)
```

Gambar 3 Optimasi Model Menggunakan GridSearchCV

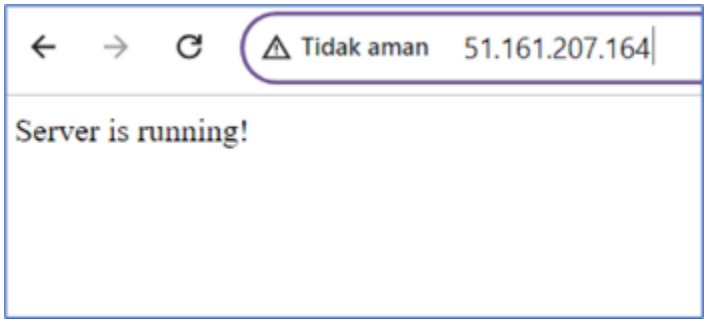
Hasil dari Algoritma Random Forest menghasilkan label “BENIGN” yang berarti tidak berbahaya dan label “DDOS” yang berarti dalam serangan DDoS. Dataset CICIDS2017 memiliki fitur sebanyak 77 fitur setelah beberapa nilai yang tidak dipakai atau nilai yang dianggap text di dalam dataset CICIDS2017. Hasil pelatihan dan ujicoba menggunakan dataset CICIDS2017 disimpan kedalam file sebagai database untuk di ujicoba langsung menggunakan VPS Cloud.

3.3 Implementasi di Lingkungan Cloud

Implementasi menggunakan Virtual Private Server atau VPS dengan Sistem Operasi Linux Ubuntu Versi 20.04. Hasil file pelatihan di transfer menggunakan Aplikasi WinScp. Konfigurasi pada server menggunakan Framework Python yaitu Flask agar dapat dijalankan di server. File yang dilatih dan disimpan kedalam file pkl yang diberinama “random_forest_ddos_model_vps_rev2.pkl”. Berikut adalah tampilan ketika server berhasil berjalan.

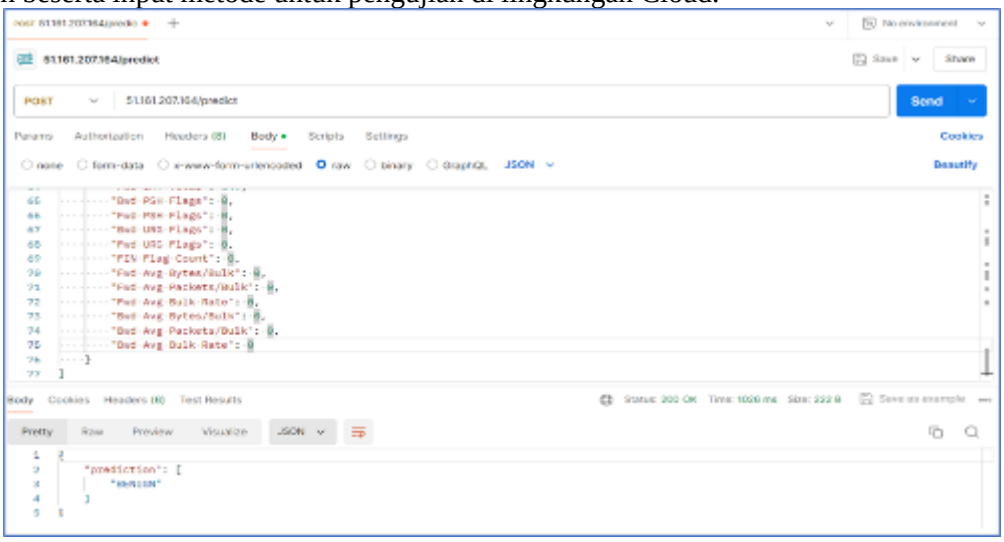
```
(venv) root@fun:/var/www/flask_app# gunicorn --bind 0.0.0.0:5000 app:app
[2024-06-26 09:48:12 +0200] [49939] [INFO] Starting gunicorn 22.0.0
[2024-06-26 09:48:12 +0200] [49939] [INFO] Listening at: http://0.0.0.0:5000 (49939)
[2024-06-26 09:48:12 +0200] [49939] [INFO] Using worker: sync
[2024-06-26 09:48:12 +0200] [49941] [INFO] Booting worker with pid: 49941
```

Gambar 4 Hasil Server yang berhasil berjalan



Gambar 5 Hasil Tampilan diakses melalui Web Browser

Selanjutnya pada tahap ujicoba menggunakan aplikasi Postman. Aplikasi Postman digunakan untuk mengganti akses Metode “Get” diubah menjadi Metode “Post” agar dapat kita ujicoba langsung dalam visualisasi serangan DDoS. Berikut adalah tampilan dari metode yang diubah beserta input metode untuk pengujian di lingkungan Cloud.



Gambar 6 Hasil dari Proses Metode Post kepada server VPS dengan pilihan point yang dapat mengganggu Server

Hasil pada gambar 9 menunjukkan sistem dapat beradaptasi dengan pelatihan menggunakan random forest karena hasil yang keluar sudah di latih sehingga masuk kedalam kelompok tidak berbahaya karena diprediksi sebagai serangan yang tidak berbahaya pada gambar 10. Sistem sudah berjalan dan terus diujicoba menggunakan data yang berbeda sehingga hasilnya tetap diprediksi sebagai tidak berbahaya.

3.4 Evaluasi Performa Model Random Forest

Untuk mengevaluasi kinerja model Random Forest dalam mendeteksi serangan Distributed Denial of Service (DDoS), kami menganalisis beberapa metrik performa penting, yaitu precision, recall, F1-score, dan akurasi. Tabel 1 menunjukkan hasil performa model Random Forest yang diperoleh dari uji coba.

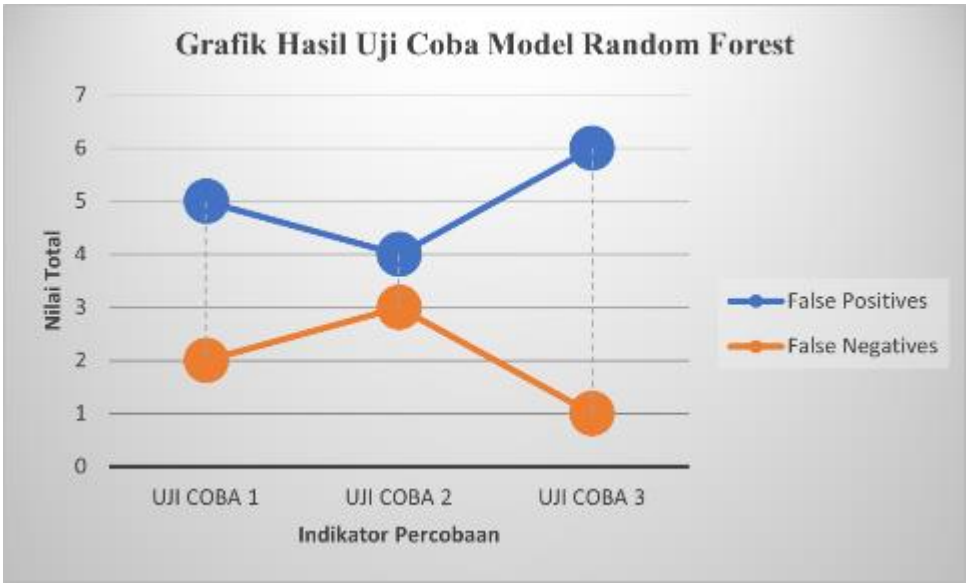
Tabel 1. Performa Model Random Forest

Metode	Precision	Recall	F1-Score	Akurasi(%)
Random Forest	0.95	0.94	0.94	98.5

Pada uji coba ini, model Random Forest menunjukkan performa yang sangat baik dalam mendeteksi serangan DDoS dibandingkan dengan teknik lainnya. Akurasi yang tinggi dan metrik performa lainnya menunjukkan efektivitas model dalam mengidentifikasi serangan DDoS dengan tingkat kesalahan yang rendah.

Tabel 2. Hasil Uji Coba Model Random Forest

Uji Coba	Serangan DDoS	Benign	False Positives	False Negatives
Uji Coba 1	1200	300	5	2
Uji Coba 2	1150	280	4	3
Uji Coba 3	1250	320	6	1



Gambar 7 Garfik hasil Percobaan Model Random Forest di Lingkungn Cloud

Dalam penelitian ini berhasil mengimplementasikan model Random Forest untuk mendeteksi serangan DDoS dengan menggunakan dataset CICIDS2017. Model ini menunjukkan performa yang memuaskan dalam mengklasifikasikan data antara serangan DDoS dan trafik normal (BENIGN). Hasil pengujian menunjukkan bahwa model Random Forest memiliki akurasi yang tinggi dalam mendeteksi serangan DDoS, dengan tingkat kesalahan yang rendah. Akurasi Model Random Forest menunjukkan akurasi sebesar 98,5% dalam mendeteksi serangan DDoS.

Kekuatan Algoritma Random Forest terbukti sangat efektif dalam menangani dataset yang besar dan kompleks seperti CICIDS2017. Kemampuan Random Forest untuk melakukan bagging dan membangun banyak pohon keputusan memungkinkan untuk menangkap berbagai pola dalam data, yang sangat penting dalam mendeteksi serangan siber yang kompleks seperti DDoS. Analisis Perilaku Pendekatan yang digunakan dalam penelitian ini tidak hanya mengandalkan fitur statis tetapi juga fitur dinamis yang berkaitan dengan perilaku jaringan, seperti waktu antar paket (IAT), ukuran segmen rata-rata, dan jumlah paket per detik. Fitur-fitur ini memainkan peran penting dalam mendeteksi pola-pola anomali yang menunjukkan adanya serangan DDoS.

Kinerja di Lingkungan Cloud implementasi model di lingkungan cloud computing menunjukkan bahwa model ini dapat diintegrasikan dengan sistem deteksi intrusi (IDS) yang ada di cloud untuk memberikan lapisan keamanan tambahan. Kinerja yang tinggi dari model ini dalam mendeteksi serangan DDoS menunjukkan bahwa penggunaan metode ini dapat membantu penyedia layanan cloud untuk melindungi infrastruktur mereka dari serangan yang merusak. Skalabilitas dan Efisiensi salah satu keunggulan dari penggunaan Random Forest adalah

skalabilitasnya. Model ini dapat diimplementasikan pada sistem cloud yang besar dan dapat menangani volume data yang tinggi tanpa mengorbankan kinerja. Selain itu, efisiensi algoritma ini dalam melakukan prediksi juga memastikan bahwa deteksi serangan dapat dilakukan secara real-time, yang merupakan aspek kritis dalam keamanan jaringan.

4. KESIMPULAN DAN SARAN

Kombinasi dari algoritma Random Forest dan analisis perilaku jaringan dapat digunakan secara efektif untuk mendeteksi serangan DDoS dalam lingkungan cloud computing. Hasil yang diperoleh dari pengujian model menunjukkan bahwa metode ini memiliki akurasi yang tinggi dan mampu membedakan dengan jelas antara trafik normal dan serangan DDoS. Dengan demikian, model ini dapat diintegrasikan ke dalam sistem keamanan jaringan untuk memberikan perlindungan yang lebih baik terhadap serangan DDoS. Penelitian lebih lanjut dapat difokuskan pada pengembangan dan pengujian model dengan menggunakan dataset yang lebih beragam serta mengoptimalkan algoritma untuk meningkatkan performa deteksi. Selain itu, penerapan model ini di lingkungan cloud yang lebih besar dan kompleks juga perlu dieksplorasi untuk memastikan skalabilitas dan efektivitasnya dalam berbagai kondisi operasional.

DAFTAR PUSTAKA

[1] A. Prayogi *et al.*, "ENHANCING NETWORK PERFORMANCE LOAD BALANCING IN CYBER CAFE NETWORKS WITH DIJKSTRA ALGORITHM ON MIKROTIK," *J. Tek. Inform.*, vol. 5, no. 1, pp. 253–261, 2024, [Online]. Available: https://jutif.if.unsoed.ac.id/index.php/jurnal/article/view/1644/448

[2] E. Barus, K. M. Pardede, and J. A. Putri Br. Manjorang, "Transformasi Digital: Teknologi Cloud Computing dalam Efisiensi Akuntansi," *J. Sains dan Teknol.*, vol. 5, no. 3, pp. 904–911, 2024, doi: 10.55338/saintek.v5i3.2862.

[3] P. Adi, D. A. Muhammad, and S. Tata, "ANALISIS PERBANDINGAN ANTARA TEKNOLOGI CLOUD COMPUTING DAN INFRASTRUKTUR KOMPUTER TRADISIONAL DALAM KONTEKS BISNIS," vol. 2, pp. 143–147, 2024.

[4] Q. A. Syahri, D. F. Waidah, and W. S. Ashari, "Perancangan Dan Implementasi Private Cloud Computing Untuk Penyimpanan Data Di Dinas Perhubungan Kabupaten Karimun," *Tikar*, vol. 5, no. 1, pp. 24–35, 2024.

[5] Y. B. M. Darkel, N. Hadi, and A. W. Rahardjo E, "Analisis QOS (Quality Of Service) Pada Bandwidth Jaringan Komputer Dengan Metode PCQ (Peer Connection Queue)," *Techno.Com*, vol. 23, no. 1, pp. 65–75, 2024, doi: 10.62411/tc.v23i1.9676.

[6] P. T. Prasetyaningrum and N. B. Hangesti, "Sistem Pakar Diagnosa Penyakit Kulit Akibat Virus Menggunakan Teorema Bayes," *Telematika*, vol. 15, no. 2, p. 117, 2018, doi: 10.31315/telematika.v15i2.3128.

[7] BSSN, "Lanskap Keamanan Siber Indonesia," no. 70, 2024.

[8] M. Juroihan, W. K. Fikri, L. Mohdo, M. Fikri, R. N. Romadhon, and M. Encep, "Integrasi Cloud Computing untuk Analisis Big Data," *Karimah Tauhid*, vol. 3, no. 4, pp. 4387–4399, 2024, doi: 10.30997/karimahtauhid.v3i4.12679.

[9] G. Wisnu *et al.*, "Tinjauan Literatur Tentang Cloud Computing dan Artificial Intelligence (AI): Potensi dan Tantangan," *Jnatia*, vol. 2, no. 2, pp. 423–428, 2024.

[10] S. M. Syifa Munawarah, Kurniabudi, and Eko Arip Winanto, "Deteksi Serangan DDoS SYN Flood Pada Jaringan Internet of Things (IoT) Menggunakan Metode Deep Neural Network (DNN)," *J. Inform. Dan Rekayasa Komputer(JAKAKOM)*, vol. 4, no. 1, pp. 982–991, 2024, doi: 10.33998/jakakom.2024.4.1.1710.

[11] Z. I. Sumayyah, S. Dimas, S. Permana, M. Tsabit, and A. Setiawan, "Penerapan dan Mitigasi Teknik Slowloris dalam Serangan Distributed Denial-of-Service (DDos) terhadap Website Ilegal dengan Kali Linux," no. 2, pp. 1–14, 2024.

[12] I. Rahmadaniar, D. Adrian, A. Tondang, B. S. Fernando, and A. Setiawan, "Implementasi Firewall Menggunakan Iptables untuk Melindungi Server dari Serangan DDoS," no. 3, pp. 1–10, 2024.

[13] D. V. Waas, M. D. W. Arsitana, I. P. H. Permana, I. K. Wiratama, and I. G. I. Sudipa, "Group Decision Support System Using SMART-COPELAND SCORE Model In Choosing The Best Alternative Pair," *Telematika*, vol. 19, no. 1, p. 117, 2022, doi: 10.31315/telematika.v19i1.7181.

[14] M. A. S. Pane, K. Saleh, A. Prayogi, R. Dian, R. M. Siregar, and R. Aris Sugianto, "Low-Cost CCTV for Home Security With Face Detection Base on IoT," *J. Inf. Syst. Technol. Res.*, vol. 3, no. 1, pp. 20–29, 2024, doi: 10.55537/jistr.v3i1.769.

[15] Suci Amaliah, M. Nusrang, and A. Aswi, "Penerapan Metode Random Forest Untuk Klasifikasi Varian Minuman Kopi di Kedai Kopi Konijiwa Bantaeng," *VARIANSI J. Stat. Its Appl. Teach. Res.*, vol. 4, no. 3, pp. 121–127, 2022, doi: 10.35580/variansiunm31.

[16] R. Supriyadi, W. Gata, N. Maulidah, and A. Fauzi, "Penerapan Algoritma Random Forest Untuk Menentukan Kualitas Anggur Merah," *E-Bisnis J. Ilm. Ekon. dan Bisnis*, vol. 13, no. 2, pp. 67–75, 2020, doi: 10.51903/e-bisnis.v13i2.247.

[17] V. Puspitasari, "Deteksi dan Respons Terhadap Ddos Attacks pada Website Dinamis," vol. 1, no. 4, pp. 18–25, 2024.