DOI: 10.22146/jnteti.v14i3.19764

Deteksi Serangan pada Jaringan IoT Menggunakan Seleksi Fitur Gabungan dan Optimasi Bayesian

Samsudiat[1], Kalamullah Ramli[1]

[1] Departemen Teknik Elektro, Fakultas Teknik, Universitas Indonesia, Depok, Jawa Barat 16424, Indonesia

[Diserahkan: 6 Maret 2025, Direvisi: 29 Mei 2025, Diterima: 6 Agustus 2025]
Penulis Korespondensi: Kalamullah Ramli (email: kalamullah.ramli@ui.ac.id)

INTISARI — Deteksi serangan berbasis *machine learning* (ML) berpotensi menjadi alternatif terbaik dalam penanganan ancaman siber pada jaringan *internet of things* (IoT). Metode ini memiliki kemampuan untuk menangani berbagai jenis serangan baru yang terus berkembang. Namun, makin banyaknya jumlah data yang dihasilkan dan penggunaan nilai-nilai parameter bawaan dari algoritma ML menyebabkan penurunan kinerja metode ini. Penelitian ini mengusulkan metode seleksi fitur gabungan (*hybrid*) yang dikombinasikan dengan optimasi Bayesian untuk meningkatkan efektivitas dan efisiensi model deteksi serangan. Metode seleksi fitur gabungan ini menggabungkan teknik filter korelasi, untuk menghapus fitur-fitur yang berkorelasi tinggi dengan cepat, dan teknik *feature importance*, untuk memilih fitur-fitur yang berpengaruh besar terhadap model. Selain itu, teknik optimasi Bayesian bertujuan menemukan nilai optimal secara efisien dari parameter-parameter algoritma ML yang tangguh dan ringan digunakan pada jaringan IoT, yaitu *decision tree* dan *random forest*. Kemudian, model yang dibangun dievaluasi menggunakan *dataset* serangan terbaru, yaitu CICIoT2023, yang terdiri atas tujuh jenis serangan, yaitu *distributed denial of service* (DDoS), *denial of service* (DoS), Mirai, *spoofing*, *reconnaissance*, serangan berbasis *website*, dan *brute force*. Hasil evaluasi menunjukkan bahwa teknik seleksi fitur gabungan menghasilkan kinerja model yang lebih efisien daripada beberapa teknik seleksi fitur tunggal dengan memilih 5 dari 46 fitur. Selain itu, teknik optimasi Bayesian juga berhasil menemukan nilai optimal dari parameter-parameter model untuk meningkatkan kinerja model pada tingkat akurasi, presisi, *recall*, dan *F*1 hingga 99,74% serta penurunan waktu komputasi hingga 97,41%. Berdasarkan hasil penelitian ini, model deteksi serangan menggunakan seleksi fitur gabungan dan optimasi Bayesian dapat menjadi rujukan dalam penerapan keamanan siber pada jaringan IoT.

KATA KUNCI — *Internet of Things*, Deteksi Serangan, *Machine Learning*, Seleksi Fitur, *Hyperparameter Optimization*, Optimasi Bayesian.

I. PENDAHULUAN

Internet of things (IoT) merupakan teknologi pengungkit pada era Revolusi Industri saat ini dan memiliki peran penting di berbagai sektor kehidupan, seperti rumah cerdas, kendaraan otonom, industri manufaktur, dan fasilitas kesehatan [1]. Istilah IoT atau biasa disebut juga dengan perangkat cerdas mengacu pada beberapa perangkat elektronik, seperti sensor, aktuator, dan objek fisik lainnya yang saling terhubung melalui internet, sehingga memungkinkan beberapa perangkat tersebut untuk menangkap, menyimpan, mengolah, dan mengirimkan data tanpa intervensi manusia [2]. Hal ini tentunya dapat memberikan kemudahan, dengan adanya otomasi pekerjaan, dan efisiensi dalam penggunaan sumber daya [3].

Pesatnya perkembangan perangkat IoT ini menyebabkan peningkatan ancaman terhadap serangan siber. Berdasarkan Lanskap Keamanan Siber Indonesia Tahun 2024, jumlah serangan siber tertinggi adalah *botnet* Mirai, yang merupakan jenis serangan yang menargetkan perangkat IoT [4]. Selain itu, beberapa kerentanan yang sering ditemukan, seperti keterbatasan sumber daya komputasi, kurangnya pembaruan perangkat lunak, dan lemahnya mekanisme keamanan, juga meningkatkan risiko terhadap serangan siber ini [5]. Serangan siber pada perangkat IoT dapat mengganggu kinerja perangkat, sehingga perangkat tidak dapat bekerja secara optimal dan bahkan dapat bekerja di luar kendali. Hal ini tentunya dapat menimbulkan kerugian, seperti kerusakan perangkat, pencurian data, serta terganggunya proses bisnis organisasi [6].

Salah satu alternatif terbaik dalam upaya penanganan ancaman terhadap serangan siber adalah dengan membangun model deteksi serangan siber berbasis pemelajaran mesin (*machine learning*, ML) [7]. Di jaringan IoT, model ini dapat diterapkan pada *intrusion detection system* (IDS) yang merupakan perangkat untuk memantau dan memeriksa paket data yang melalui internet serta memberikan peringatan jika terdapat paket data yang mencurigakan [8]. IDS memiliki peran penting dalam jaringan IoT karena memiliki kemampuan untuk menghadapi jenis-jenis serangan siber baru yang terus berkembang. Akan tetapi, seiring berjalannya waktu, makin banyak jumlah data yang dihasilkan, sehingga menyebabkan penurunan kinerja dari model ini [9]. Peningkatan dimensi data serangan siber menyebabkan peningkatan kompleksitas model dan penggunaan sumber daya komputasi. Selain itu, nilai-nilai parameter bawaan dari model ML yang digunakan juga menyebabkan kinerja model menjadi kurang optimal [10]. Oleh karena itu, teknik seleksi fitur dan *hyperparameter optimization* (HPO) dibutuhkan untuk meningkatkan kinerja model deteksi serangan siber pada jaringan IoT.

Berdasarkan permasalahan tersebut, beberapa penelitian telah mengusulkan metode berbasis ML untuk meningkatkan kinerja model deteksi serangan siber pada jaringan IoT, salah satunya adalah dengan mengembangkan *dataset* serangan siber, yaitu CICIoT2023 [11]. CICIoT2023 merupakan *dataset* terbaru yang dihasilkan dengan menjalankan tujuh jenis serangan yang berbeda pada jaringan IoT yang terdiri atas 105 perangkat yang berbeda. Kemudian, data yang diperoleh dievaluasi menggunakan beberapa algoritma ML. Hasil evaluasi menunjukkan bahwa algoritma *random forest* (RF) menghasilkan tingkat akurasi yang paling tinggi, yaitu mencapai 99,68%. Meskipun demikian, penelitian ini tidak mengevaluasi efisiensi penggunaan sumber daya komputasi.

Penelitian lain yang menggunakan *dataset* ini juga telah membangun model deteksi serangan siber menggunakan tiga algoritma *deep learning* (DL), yaitu *deep neural network* (DNN), *convolutional neural network* (CNN), dan *long short-term memory* (LSTM) [12]. Hasil penelitian menunjukkan bahwa algoritma CNN mencapai hasil yang paling tinggi dengan tingkat akurasi 99,40% dan waktu komputasi 618 s untuk model klasifikasi biner serta tingkat akurasi 99,10% dan waktu komputasi 767 s untuk model klasifikasi multikelas. Kemudian, penelitian lainnya menggunakan model klasifikasi gabungan yang menggabungkan algoritma *decision tree* (DT), RF, dan *gradient boosting* [13]. Hasil penelitian menunjukkan bahwa model gabungan ini mencapai tingkat akurasi 99,51% dan waktu komputasi 448 s. Sementara itu, penelitian lainnya yang memanfaatkan model klasifikasi gabungan juga dilakukan dengan mengombinasikan tiga algoritma DL, yaitu *auto-encoder* (AE), LSTM, dan CNN [14]. Hasil penelitian menunjukkan bahwa model gabungan ini mencapai tingkat akurasi 99,15% dan rata-rata waktu komputasi 150 s untuk setiap siklus pelatihan. Meskipun ketiga penelitian ini telah menghasilkan tingkat akurasi yang tinggi, yaitu mencapai lebih dari 99%, tetapi waktu komputasi yang dibutuhkan juga masih tinggi, yaitu lebih dari 2 min.

Kemudian, pada penelitian penggunaan seleksi fitur, beberapa metode seperti filter, *wrapper*, dan *embedded* telah digunakan [15]-[17]. Masing-masing metode tersebut memiliki kelebihan dan kekurangan. Metode filter unggul dalam waktu komputasi yang lebih cepat, tetapi tidak mempertimbangkan kinerja dan interaksi antarfitur. Metode *wrapper* unggul dalam tingkat akurasi yang lebih tinggi, tetapi membutuhkan waktu komputasi yang lebih lama, sedangkan metode *embedded* unggul dalam waktu komputasi yang lebih cepat dan tingkat akurasi yang lebih tinggi, tetapi terbatas hanya pada beberapa algoritma tertentu. Oleh karena itu, metode seleksi fitur gabungan diusulkan untuk menggabungkan keunggulan masing-masing metode seleksi fitur tersebut.

Penelitian penggunaan teknik seleksi fitur gabungan telah dilakukan dengan menggabungkan dua metode filter, yaitu teknik varians dan korelasi, untuk mendeteksi serangan *botnet* pada jaringan IoT [18]. Metode seleksi fitur ini memilih 14 fitur terbaik dengan hasil penelitian menunjukkan bahwa algoritma DT mencapai tingkat akurasi 100% dan waktu komputasi 15,85 s, sedangkan algoritma *naïve Bayes* mencapai tingkat akurasi 99,29% dan waktu komputasi 2,10 s. Penelitian lainnya yang juga menggunakan teknik seleksi fitur gabungan telah menggabungkan teknik *minimum redundancy maximum relevance* (MRMR) dan *principal component analysis* (PCA) untuk mendeteksi serangan *distributed denial of service* (DDoS) pada jaringan IoT [19]. Metode seleksi fitur ini memilih sepuluh fitur terbaik dengan hasil penelitian menunjukkan bahwa model deteksi mencapai tingkat akurasi 99,90% dan waktu komputasi 60,817 s. Kedua penelitian ini telah mencapai tingkat akurasi yang tinggi dengan waktu komputasi yang rendah, tetapi hanya berfokus pada jenis serangan tertentu.

Selain teknik seleksi fitur, kinerja model juga bergantung pada pemilihan nilai-nilai parameter algoritma ML dan beberapa penelitian teknik HPO telah banyak digunakan. Algoritma genetika telah digunakan sebagai teknik seleksi fitur dan HPO pada algoritma RF dan eXtreme Gradient Boosting (XGBoost) untuk mendeteksi serangan *port scan* dan DDoS pada jaringan IoT [20]. Hasil penelitian menunjukkan bahwa model RF mencapai tingkat akurasi 96,36% dan waktu komputasi 31,24 s, sedangkan model XGBoost mencapai tingkat akurasi 96,36% dan waktu komputasi 1,82 s. Meskipun hasil penelitian menunjukkan efisiensi penggunaan sumber daya komputasi yang tinggi, tetapi tingkat akurasi yang dihasilkan masih rendah. Kemudian, penelitian lainnya menggunakan optimasi Bayesian pada model AE dan DNN [21]. Hasil penelitian menunjukkan bahwa model deteksi mencapai tingkat akurasi yang tinggi, yaitu 99,99%, tetapi waktu komputasi yang dibutuhkan juga tinggi, yaitu 232,393 s.

Berdasarkan kajian beberapa penelitian sebelumnya, penelitian telah berhasil membangun model deteksi serangan siber berbasis ML yang mencapai tingkat akurasi yang tinggi, yaitu lebih dari 90%. Meskipun demikian, masih terdapat ruang untuk meningkatkan tingkat akurasi tersebut sambil menurunkan tingkat penggunaan sumber daya. Oleh karena itu, penelitian ini mengusulkan teknik seleksi fitur gabungan yang menggabungkan filter korelasi dan *feature importance* serta teknik optimasi Bayesian untuk meningkatkan kinerja model deteksi serangan siber berbasis ML. Filter korelasi bertujuan untuk menghapus fitur-fitur yang berkorelasi tinggi dengan cepat, sedangkan *feature importance* bertujuan untuk memilih fitur-fitur yang berpengaruh besar terhadap model. Kemudian, optimasi Bayesian bertujuan untuk menemukan nilai optimal dari parameter-parameter algoritma ML yang tangguh dan ringan digunakan pada jaringan IoT, yaitu DT dan RF. Metode yang diusulkan dievalusi menggunakan *dataset* serangan siber terbaru, yaitu CICIoT2023. Hasil penelitian ini diharapkan dapat menjadi alternatif terbaik dalam penerapan keamanan siber terutama pada jaringan IoT.

Makalah ini disusun sebagai berikut. Bagian II membahas tentang konsep serangan siber pada jaringan IoT, deteksi serangan siber berbasis ML, *dataset* CICIoT2023, seleksi fitur, dan HPO. Bagian III membahas tentang tahapan-tahapan penelitian membangun model ML untuk mendeteksi serangan siber pada jaringan IoT. Kemudian, hasil penelitian dibahas dan dievaluasi pada Bagian IV, yang terdiri atas analisis kinerja model dengan teknik seleksi fitur gabungan dan optimasi Bayesian. Terakhir, kesimpulan dan saran dari keseluruhan penelitian ini disampaikan pada Bagian V.

II. MODEL DETEKSI SERANGAN

A. SERANGAN SIBER PADA JARINGAN IoT

Istilah IoT pertama kali dicetuskan pada tahun 1999 oleh Kevin Ashton, seorang inovator teknologi yang bekerja di sebuah perusahaan yang bergerak di bidang *radio frequency identification* (RFID) [22]. Teknologi RFID dapat digunakan untuk menghubungkan berbagai objek fisik atau "*things*" ke internet, sehingga memungkinkan pengumpulan dan pertukaran data antara objek-objek fisik tersebut. Namun, makin banyak objek fisik yang terhubung dengan internet, makin tinggi risiko terhadap serangan siber.

Serangan siber merupakan suatu tindak kejahatan oleh seseorang atau sekelompok orang yang dapat menurunkan tingkat kerahasiaan, integritas, atau ketersediaan informasi [23]. Bentuk-bentuk tindakan ini dapat berupa pengaksesan sistem secara tidak sah, pencurian, manipulasi, dan bahkan perusakan data pada sistem dan jaringan komputer target. Tujuan dari serangan ini bervariasi, mulai dari pencurian informasi sensitif hingga mengganggu operasional bisnis organisasi, yang dapat menyebabkan kerugian finansial, reputasi, atau bahkan hukum.

Terdapat berbagai jenis serangan siber. Salah satu jenis yang sering terjadi pada jaringan IoT adalah *botnet* [24]. *Botnet* merupakan *malicious software* (*malware*) yang dapat menginfeksi beberapa perangkat IoT, sehingga dapat dikendalikan

oleh penyerang dari jarak jauh untuk dapat melancarkan kembali serangan yang lebih besar, seperti DDoS [25]. DDoS merupakan serangan yang dapat membanjiri server target dengan banyak lalu lintas (*traffic*) yang melebihi kemampuannya, sehingga layanan menjadi *overload* dan tidak tersedia. Hal ini tentunya dapat mengganggu operasional bisnis organisasi. Selain *botnet* dan DDoS, masih ada jenis serangan lain pada jaringan IoT, di antaranya *brute force*, *spoofing*, *man in the middle*, serta serangan berbasis web seperti *backdoor* dan *command injection* [26].

B. DETEKSI SERANGAN BERBASIS MACHINE LEARNING

ML merupakan bagian dari kecerdasan buatan yang merupakan suatu komputer atau "*machine*" yang dapat mempelajari data atau "*learning*" dengan algoritma tertentu tanpa diprogram secara khusus [27]. Berbeda dengan program komputer konvensional yang bergantung pada instruksi manusia, komputer ini dapat melakukan identifikasi pola data, sehingga mampu memberikan prediksi atau keputusan. ML bertujuan untuk meningkatkan kemampuan komputer dalam melakukan suatu tugas tertentu dalam rangka membantu sebagian pekerjaan manusia.

Model klasifikasi merupakan salah satu cabang dari ML yang berfungsi untuk mengelompokkan data ke dalam kelas atau kategori tertentu berdasarkan fitur-fiturnya. Deteksi serangan siber pada jaringan IoT dapat dibangun dengan menggunakan model klasifikasi yang biasanya diterapkan pada perangkat IDS [28]. IDS merupakan perangkat yang berfungsi untuk memantau dan mendeteksi aktivitas paket-paket data yang melalui internet serta memberikan peringatan jika terdapat aktivitas mencurigakan. Cara kerja IDS adalah dengan membandingkan karakteristik paket data yang melintas dengan karakteristik paket data yang dianggap normal. Terdapat dua pendekatan dalam metode deteksi IDS, yaitu *signature* dan anomali. Pada metode *signature*, paket data dibandingkan dengan basis data serangan yang telah teridentifikasi. Basis data serangan ini biasanya disediakan oleh komunitas atau penyedia jasa layanan keamanan siber. Sementara itu, pada metode anomali, paket data dibandingkan dengan pola data sebelumnya yang dianggap normal secara statistik. Metode anomali ini memiliki keunggulan karena mampu mengidentifikasi jenis-jenis serangan baru yang tidak terdapat dalam basis data metode *signature* dengan menggunakan model klasifikasi. Model klasifikasi digunakan untuk mengidentifikasi paket data berdasarkan karakteristik fitur-fiturnya, seperti ukuran paket, jumlah paket, dan kecepatan paket.

Model deteksi serangan siber pada jaringan IoT memiliki beberapa karakteristik yang khas dibandingkan dengan model pada jaringan komputer pada umumnya [29]. Pertama, perangkat IoT terhubung langsung ke lingkungan fisik, sehingga rentan terkena serangan fisik. Kedua, jenis perangkat IoT lebih banyak daripada jenis perangkat komputer, sehingga kompleksitas jaringan lebih besar karena memiliki banyak variasi protokol dan media komunikasi. Ketiga, perangkat IoT memiliki sumber daya komputasi yang rendah, sehingga mekanisme keamanannya lebih terbatas dibandingkan dengan perangkat komputer. Oleh karena itu, model deteksi serangan yang dibangun pada jaringan IoT harus memiliki karakteristik yang tangguh dan ringan. Beberapa algoritma model klasifikasi yang tangguh dan ringan yang digunakan pada penelitian ini adalah sebagai berikut.

1) *DECISION TREE (DT)*

DT merupakan algoritma yang membangun model pembelajaran seperti struktur pohon yang terdiri atas akar, cabang, dan daun [30]. Setiap akar yang mewakili fitur-fitur pada *dataset* dipilih berdasarkan fitur yang paling informatif dengan menggunakan kriteria tertentu, seperti *gini* atau *entropy*. Kemudian, setiap akar akan membentuk suatu cabang, yang mewakili aturan keputusan, untuk membentuk daun, yang mewakili hasil akhir keputusan, berdasarkan nilai kelas. Proses ini diulang secara rekursif hingga mencapai kriteria untuk berhenti, seperti kedalaman maksimum pohon atau jumlah sampel minimum.

Algoritma DT memiliki kelebihan pada kemudahan interpretasinya, sehingga ringan untuk diimplementasikan pada perangkat yang memiliki sumber daya komputasi terbatas, seperti pada perangkat IoT. Selain itu, algoritma ini juga terkenal memiliki kinerja yang baik dalam membangun model deteksi serangan siber [31]. Di sisi lain, kelemahan algoritma ini adalah rentan terhadap *overfitting*, yaitu model terlalu baik dalam mempelajari data, sehingga dapat menurunkan tingkat akurasi pada data baru yang belum pernah dipelajari.

2) *RANDOM FOREST (RF)*

RF merupakan algoritma yang menggabungkan kekuatan dari beberapa pohon algoritma DT untuk menghasilkan kinerja yang lebih baik [32]. Setiap pohon dibangun dengan menggunakan subset data dan fitur yang berbeda secara acak. Tujuannya adalah untuk mengurangi risiko *overfitting* pada algoritma DT tunggal. Kemudian, masing-masing pohon memberikan hasil keputusan dan pengambilan keputusan akhir ditentukan dengan suara terbanyak, yaitu memilih nilai keputusan yang paling sering muncul.

Algoritma RF memiliki kelebihan pada kemampuannya dalam menangani data berdimensi besar dengan kinerja yang tinggi, seperti data serangan siber [33]. Selain itu, algoritma ini juga mampu menangani *outlier* dan derau pada data. *Outlier* adalah data yang memiliki nilai yang berbeda secara signifikan dalam *dataset*, sedangkan derau adalah data yang tidak relevan, seperti tidak konsisten atau tidak lengkap. Kelemahan algoritma ini adalah membutuhkan sumber daya komputasi yang lebih besar untuk membangun beberapa pohon algoritma DT.

C. DATASET CICIoT2023

Dataset CICIoT2023 merupakan *dataset* serangan siber pada jaringan IoT yang diterbitkan oleh Canadian Institute for Cyber-security (CIC), University of New Brunswick (UNB), Kanada pada tahun 2023 [34]. *Dataset* ini dibangun dengan menjalankan 33 jenis serangan ke beberapa perangkat IoT yang menghasilkan 46.686.579 data yang telah dievaluasi dan digunakan oleh banyak peneliti di dunia. Jenis-jenis serangan pada *dataset* ini dikelompokkan menjadi tujuh kelas serangan, yaitu DDoS, *denial of service* (DoS), Mirai, *reconnaissance*, *brute force*, *spoofing*, dan serangan berbasis *website* dengan jumlah data masing-masing serangan ditampilkan pada Tabel I.

Terdapat tiga jenis fitur pada *dataset* ini, yaitu fitur berbasis waktu, fitur berbasis lalu lintas, dan fitur statistik, yang berjumlah 46 fitur dan ditampilkan pada Tabel II. Fitur berbasis waktu mencakup informasi tentang waktu terjadinya suatu aktivitas dan fitur berbasis lalu lintas mencakup informasi tentang karakteristik trafik paket data. Sementara itu, fitur statistik berisi nilai-nilai statistik dari karakteristik beberapa paket data dalam satu aliran yang sama.

D. SELEKSI FITUR

Seleksi fitur merupakan proses pengurangan dimensi data dengan memilih dan/atau menghapus beberapa fitur melalui suatu teknik tertentu [35]. Tujuan utama dari proses ini adalah

TABEL I
JUMLAH DATA SETIAP KELAS *DATASET* CICIoT2023

Kelas	Jumlah
DDoS	33.984.560
DoS	8.090.738
Mirai	2.634.124
Benign	1.098.195
Spoofing	486.504
Reconnaissance	354.565
Web-based	24.829
Brute force	13.064
Total	46.686.579

TABEL II
FITUR-FITUR PADA *DATASET* CICIoT2023

***Dataset* CICIoT2023**	**Fitur**
6 fitur berbasis waktu	Flow_Duration, Duration, Rate, Srate, Drate, IAT
28 Fitur berbasis lalu lintas	Header_Length, Protocol_Type, FIN_Flag, SYN_Flag, RST_Flag, PSH_Flag, ACK_Flag, ECE_Flag, CWR_Flag, ACK_Count, SYN_Count, FIN_Count, URG_Count, RST_Count, HTTP, HTTPS, DNS, Telnet, SMTP, SSH, IRC, TCP, UDP, DHCP, ARP, ICMP, IPv, LLC
12 fitur statistik	Tot_Sum, Min, Max, Avg, Std, Tot_Size, Number, Magnitude, Radius, Covariance, Variance, Weight

untuk menurunkan kompleksitas dan tingkat penggunaan sumber daya komputasi, sehingga dapat meningkatkan kinerja model ML. Selain itu, proses ini juga dapat mengurangi risiko *overfitting* dan mempermudah interpretasi model. Secara umum, terdapat tiga metode seleksi fitur, yaitu filter, *wrapper*, dan *embedded*. Metode filter adalah metode yang memilih fitur berdasarkan peringkat nilai fitur yang dihitung secara statistik, sedangkan metode *wrapper* adalah metode yang memilih fitur berdasarkan peringkat nilai fitur yang dihitung dari hasil pembelajaran model, seperti RF. Terakhir, metode *embedded* memilih fitur pada saat membangun model, seperti *feature importance*. Beberapa teknik yang digunakan untuk melakukan seleksi fitur pada penelitian ini adalah sebagai berikut.

1) FILTER KORELASI

Dalam ilmu statistika, korelasi merupakan ukuran hubungan antara dua variabel yang berbeda. Rentang nilai korelasi adalah antara -1, yang menunjukkan hubungan berbanding terbalik yang sempurna, hingga +1, yang menunjukkan hubungan berbanding lurus yang sempurna [36]. Pada rentang nilai tersebut, terdapat lima sifat korelasi, yaitu korelasi sangat rendah pada nilai 0–0,2; korelasi rendah pada nilai 0,2–0,4; korelasi sedang pada nilai 0,4–0,6; korelasi tinggi pada nilai 0,6–0,8; dan korelasi sangat tinggi pada nilai 0,8–1. Salah satu jenis korelasi yang umum digunakan pada model ML adalah korelasi Pearson, yang menghitung nilai korelasi secara linier dengan menggunakan (1).

$$r = \frac{\sum[(X-\bar{X})(Y-\bar{Y})]}{\sqrt{[\sum(X-\bar{X})^2 \sum(Y-\bar{Y})^2]}} \quad (1)$$

dengan r adalah nilai korelasi; X, Y adalah nilai variabel X dan Y ke-i; dan $\bar{X}, \bar{Y}$ adalah rata-rata nilai pada variabel X dan Y.

Pada model ML, fitur-fitur *dataset* yang berkorelasi sangat tinggi tidak memberikan informasi tambahan terhadap model. Seleksi fitur dengan teknik filter korelasi akan menghapus fitur-fitur yang berkorelasi sangat tinggi tersebut, yaitu pada nilai ambang batas 0,8. Teknik ini dapat menghilangkan sifat multikolinearitas, yaitu ketidakstabilan model ML akibat adanya fitur yang redundan. Selain itu, teknik ini dapat bekerja dengan cepat karena hanya menggunakan perhitungan statistik tanpa pembelajaran algoritma ML.

2) *FEATURE IMPORTANCE*

Pada saat membangun model menggunakan algoritma DT atau RF, fitur-fitur pada *dataset* dipilih berdasarkan fitur yang paling informatif, sehingga secara implisit, algoritma ini telah melakukan seleksi fitur [37]. Nilai untuk mengukur fitur-fitur yang paling informatif tersebut adalah *feature importance*, yang dihitung dengan menggunakan konsep entropi. Entropi merupakan ukuran homogenitas atau ketidakteraturan data dengan rentang nilai antara 0 hingga 1. Nilai mendekati 0 menunjukkan data yang relatif homogen, sedangkan nilai mendekati 1 menunjukkan data yang relatif beragam. Nilai entropi dapat diperoleh menggunakan (2).

$$S = -\sum_{i=1}^{c} p_i \log_2 p_i \quad (2)$$

dengan p_i adalah proporsi jumlah elemen dari kelas ke-i dalam ruang sampel S dan c adalah jumlah kelas.

Setelah nilai *feature importance* diperoleh, fitur-fitur diurutkan dari nilai yang tertinggi ke yang terendah. Kemudian, seleksi fitur dilakukan dengan memilih beberapa fitur teratas. Keunggulan utama dari teknik ini yaitu beberapa fitur yang dipilih adalah fitur-fitur yang pasti relevan terhadap model ML. Selain itu, teknik ini dapat menangani hubungan nonlinier antarfitur yang tidak dapat dilakukan oleh teknik filter korelasi.

3) SELEKSI FITUR GABUNGAN

Masing-masing teknik seleksi fitur tersebut memiliki kelebihan dan kekurangan. Teknik seleksi fitur gabungan dibangun dengan tujuan untuk menggabungkan kelebihan dan menangani kekurangan dari teknik seleksi fitur tunggal. Penelitian ini menggunakan teknik filter korelasi pada tahap pertama seleksi fitur karena mampu memilih subset fitur dengan menghapus beberapa fitur yang redundan secara cepat. Kemudian, tahap kedua menggunakan teknik *feature importance* untuk memilih subset fitur yang memiliki nilai paling informatif terhadap model. Kombinasi dari kedua teknik ini diharapkan mampu menurunkan dimensi data dengan meningkatkan kinerja model deteksi serangan siber pada jaringan IoT.

E. HYPERPARAMETER OPTIMIZATION (HPO)

Setiap algoritma ML memiliki beberapa parameter yang nilainya dapat ditentukan sebelum proses pelatihan dilakukan atau biasa disebut dengan *hyperparameter*. HPO adalah proses pencarian nilai-nilai *hyperparameter* yang optimal dari suatu algoritma ML [38]. Proses ini bertujuan untuk menemukan kombinasi nilai-nilai *hyperparameter* yang mampu meningkatkan kinerja dan generalisasi model. Selain itu, proses ini dapat meningkatkan efisiensi pelatihan model tanpa dilakukannya penyetelan nilai-nilai *hyperparameter* secara manual. Beberapa teknik HPO yang sering digunakan antara lain *grid search*, *random search*, dan optimasi Bayesian.

Optimasi Bayesian adalah teknik HPO yang menggunakan model probabilistik untuk mencari nilai terbaik dari hasil pencarian sebelumnya. Model probabilistik dibangun dari fungsi objektif menggunakan proses Gaussian (*Gaussian process*, GP) untuk memprediksi nilai fungsi pada titik-titik

yang belum dievaluasi. Berdasarkan hasil prediksi GP, fungsi akuisisi digunakan untuk memilih titik evaluasi berikutnya. Teknik ini lebih efisien karena hanya berfokus pada ruang pencarian yang lebih menjanjikan daripada kedua teknik lainnya yang melakukan pencarian dengan mencoba banyak kombinasi.

III. METODOLOGI

Secara umum, penelitian ini terdiri atas tiga tahapan untuk membangun model deteksi berbasis ML, yaitu persiapan data, seleksi fitur, dan evaluasi model.

A. PERSIAPAN DATA

Persiapan data merupakan tahapan pertama dalam membangun model klasifikasi yang mentransformasikan data mentah menjadi data dengan format yang sesuai dan siap digunakan untuk pembelajaran model ML. Tahapan ini bertujuan untuk meningkatkan kualitas data sebelum dilakukan pengolahan dan analisis lebih lanjut. Beberapa proses dari tahapan ini yaitu pembersihan data, kodifikasi, penyeimbangan kelas, dan normalisasi.

Pembersihan data dilakukan melalui penanganan terhadap data duplikat, kosong, tidak terdefinisi, dan inkonsisten. Berdasarkan pengecekan, tidak terdapat data duplikat, kosong, dan tidak terdefinisi, tetapi terdapat tiga fitur yang hanya memiliki nilai 0, yaitu Telnet, SMTP, dan IRC. Karena fitur yang hanya memiliki nilai 0 tidak akan memengaruhi model ML, ketiga fitur tersebut dihapus, sehingga hasil akhir proses ini adalah *dataset* yang memiliki 43 fitur.

Kemudian, kodifikasi data dilakukan dengan mengubah nilai label *Benign* sebagai data normal menjadi nilai 0 dan nilai label lainnya sebagai data serangan menjadi nilai 1. Tujuan dari perubahan ke kode angka ini adalah agar model ML dapat lebih mudah memahami data. Hasil akhir proses ini adalah *dataset* dengan label data bernilai 0 berjumlah 1.098.195 dan label data bernilai 1 berjumlah 45.588.384, yang berasal dari penjumlahan data tujuh jenis serangan.

Berdasarkan hasil kodifikasi, diketahui bahwa terdapat ketidakseimbangan distribusi label data. Hal ini dapat menyebabkan model menjadi bias, yaitu model cenderung sering memprediksi kelas mayoritas daripada kelas minoritas. Oleh karena itu, penyeimbangan kelas dilakukan dengan menggunakan teknik *random undersampling* yang menghapus beberapa data pada kelas mayoritas secara acak hingga berjumlah sama dengan kelas minoritas. Teknik ini memiliki keunggulan dalam hal efisiensi penggunaan sumber daya komputasi, terutama pada *dataset* serangan siber yang biasanya memiliki dimensi data yang besar [39]. Selain itu, teknik ini juga menghilangkan risiko duplikasi data yang mungkin terjadi pada teknik *oversampling*. Hasil akhir proses ini adalah *dataset* dengan jumlah data 0 dan data 1 yang seimbang, yaitu masing-masing berjumlah 1.098.195, sehingga keseluruhan data berjumlah 2.196.390.

Terakhir, normalisasi dilakukan untuk mengubah skala nilai dari masing-masing fitur agar memiliki rentang yang sama. Hal ini bertujuan untuk menghindari dominasi fitur, sehingga masing-masing fitur memiliki pengaruh yang seimbang terhadap model ML [40]. Pada penelitian ini, normalisasi dilakukan dengan teknik *min-max*, yaitu mengubah nilai-nilai fitur dalam rentang antara 0 hingga 1, yang dapat dihitung dengan menggunakan (3).

$$X_{normalisasi} = \frac{X_{awal} - min(X)}{max(X) - min(X)}. \quad (3)$$

TABEL III
RENTANG NILAI PARAMETER ALGORITMA DT DAN RF

Parameter	Deskripsi	Rentang Nilai
criterion	Kriteria untuk memilih fitur yang akan digunakan di setiap simpul	*gini, entropy*
max_depth	Kedalaman maksimum pohon	2 – 10
min_samples_split	Jumlah sampel minimum yang dibutuhkan untuk memisahkan simpul	2 – 5
min_samples_leaf	Jumlah sampel minimum yang harus ada pada setiap daun	2 – 5
n_estimators	Jumlah pohon keputusan yang digunakan dalam algoritma *random forest*	10 – 100

B. PEMBANGUNAN MODEL DETEKSI SERANGAN

Tahapan selanjutnya adalah membangun model deteksi serangan siber yang terdiri atas seleksi fitur, pembagian data, dan pelatihan model. Seleksi fitur merupakan proses awal pada tahapan ini, yang bertujuan untuk memilih fitur-fitur yang paling informatif, dengan menggunakan teknik seleksi fitur gabungan yang menggabungkan filter korelasi dan *feature importance*. Kemudian, data hasil seleksi fitur dibagi secara acak menjadi data latih berjumlah 80% dan data uji berjumlah 20%. Terakhir, data latih tersebut akan digunakan untuk melatih model ML dengan teknik optimasi Bayesian pada algoritma DT dan RF, sedangkan data uji akan digunakan untuk mengevaluasi model ML. Ruang pencarian nilai parameter-parameter pada algoritma DT dan RF yang digunakan untuk optimasi Bayesian ditampilkan pada Tabel III.

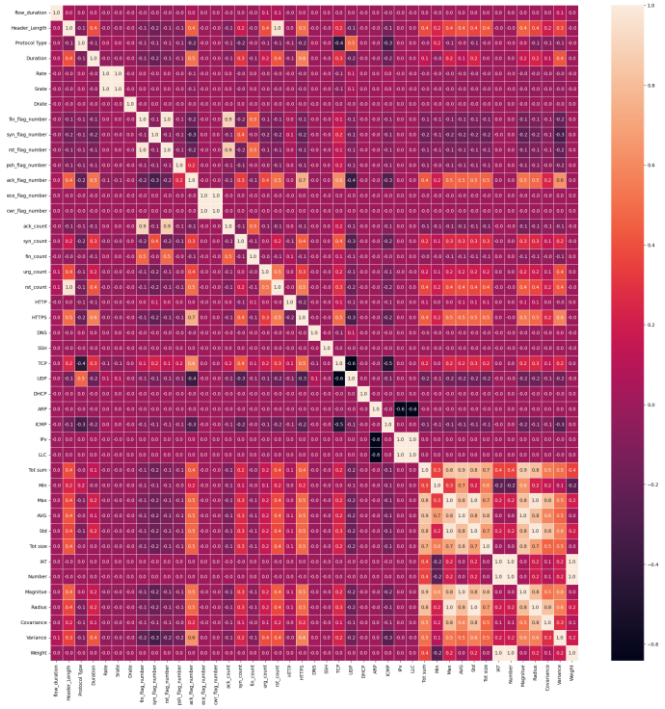
C. EVALUASI MODEL

Evaluasi model bertujuan untuk mengukur kinerja model ML yang telah dilatih dalam melakukan prediksi pada data baru yang belum pernah dilatih sebelumnya. Pada model klasifikasi, evaluasi model dilakukan dengan menggunakan *confusion matrix*, yaitu tabel berukuran $n \times n$ yang merepresentasikan jumlah kelas yang berisi nilai kelas hasil prediksi dengan nilai kelas sesungguhnya. Elemen-elemen pada *confusion matrix* adalah *true positive* (TP), yang menunjukkan jumlah data positif yang diprediksi sebagai positif; *true negative* (TN), yang menunjukkan jumlah data negatif yang diprediksi sebagai negatif; *false positive* (FP), yang menunjukkan jumlah data negatif yang diprediksi sebagai positif; dan *false negative* (FN), yang menunjukkan jumlah data positif yang diprediksi sebagai negatif. Berdasarkan elemen-elemen tersebut, interpretasi evaluasi model dapat dilakukan menggunakan metrik-metrik pada (4) hingga (7).

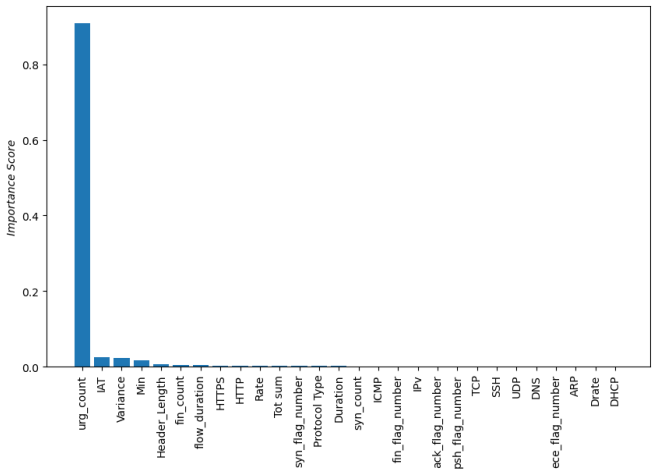
Persamaan (4) merupakan metrik akurasi, yang merupakan perbandingan antara jumlah sampel yang diprediksi benar dengan jumlah sampel keseluruhan.

$$Akurasi = \frac{TP+TN}{TP+TN+FP+FN}. \quad (4)$$

Persamaan (5) merupakan metrik presisi, yang merupakan perbandingan antara jumlah serangan yang diprediksi benar dengan keseluruhan jumlah serangan yang diprediksi. Metrik ini menunjukkan efektivitas model dalam tingkat ketepatan untuk memprediksi serangan siber.



Gambar 1. Matriks korelasi.



Gambar 2. Pengukuran *feature importance*.

$$Presisi = \frac{TP}{TP+FP}. \quad (5)$$

Persamaan (6) merupakan metrik *recall*, yang merupakan perbandingan antara jumlah serangan yang diprediksi benar dengan keseluruhan jumlah serangan yang aktual. Metrik ini menunjukkan sensitivitas model dalam tingkat kesalahan untuk mencegah serangan siber yang sesungguhnya yang tidak terdeteksi.

$$Recall = \frac{TP}{TP+FN}. \quad (6)$$

Persamaan (7) merupakan metrik *F*1, yang merupakan kombinasi antara presisi dan *recall*. Metrik ini menunjukkan kinerja dan keseimbangan model dalam memprediksi paket data.

$$F1 = \frac{2\ x\ Presisi\ x\ Recall}{Presisi+Recall}. \quad (7)$$

Terakhir, waktu komputasi adalah waktu yang dibutuhkan untuk melatih dan menguji model, yang menunjukkan efisiensi model.

TABEL IV
PERBANDINGAN KINERJA SELEKSI FITUR TUNGGAL DENGAN GABUNGAN

Metode	Jumlah Fitur	Akurasi (%)	Waktu Komputasi (s)	Pengurangan Waktu (%)
Semua fitur	43	99,56	56,20	-
Filter korelasi	28	99,55	31,16	44,56
Mutual information	10	99,36	13,27	76,39
Chi square	10	98,68	14,89	73,51
recursive Feature elimination	10	99,52	18,50	67,08
Feature importance	5	99,46	11,19	80,09
Seleksi fitur gabungan	5	99,37	7,20	87,19

TABEL V
NILAI PARAMETER TERBAIK ALGORITMA DT DAN RF

Parameter	Rentang Nilai	Nilai Terbaik DT	Nilai Terbaik RF
criterion	*gini, entropy*	*gini*	*entropy*
max_depth	2 – 10	10	10
min_samples_split	2 – 5	2	2
min_samples_leaf	2 – 5	2	2
n_estimators	10 – 100	-	28

IV. HASIL DAN PEMBAHASAN

Model deteksi serangan siber pada penelitian ini dibangun pada perangkat keras prosesor Intel Xeon 3,5 GHz dan RAM 64 GB, sedangkan perangkat lunak yang digunakan adalah Jupyter Notebook v.7.2.2 dengan bahasa pemrograman Python v.3.12.7. Beberapa pustaka yang digunakan yaitu Pandas untuk persiapan data, Matplotlib untuk visualisasi data, scikit-learn untuk membangun dan mengevaluasi model ML, serta scikit-optimize untuk melakukan optimasi Bayesian.

A. HASIL SELEKSI FITUR GABUNGAN

Teknik filter korelasi merupakan tahap pertama dari tahapan seleksi fitur, yang bertujuan untuk menghapus fitur-fitur yang memiliki korelasi tinggi dengan cepat. Teknik ini dilakukan dengan menghitung nilai korelasi 43 fitur hasil dari tahapan persiapan data. Gambar 1 menampilkan matriks korelasi yang dibangun, dengan warna elemen yang makin terang menunjukkan bahwa nilai korelasi makin tinggi. Penelitian ini menggunakan ambang batas nilai korelasi sebesar 0,8 dan terdapat 15 fitur yang memiliki nilai korelasi di atas ambang batas tersebut yang dihapus. Hasil dari tahap ini adalah *dataset* dengan 28 fitur terpilih.

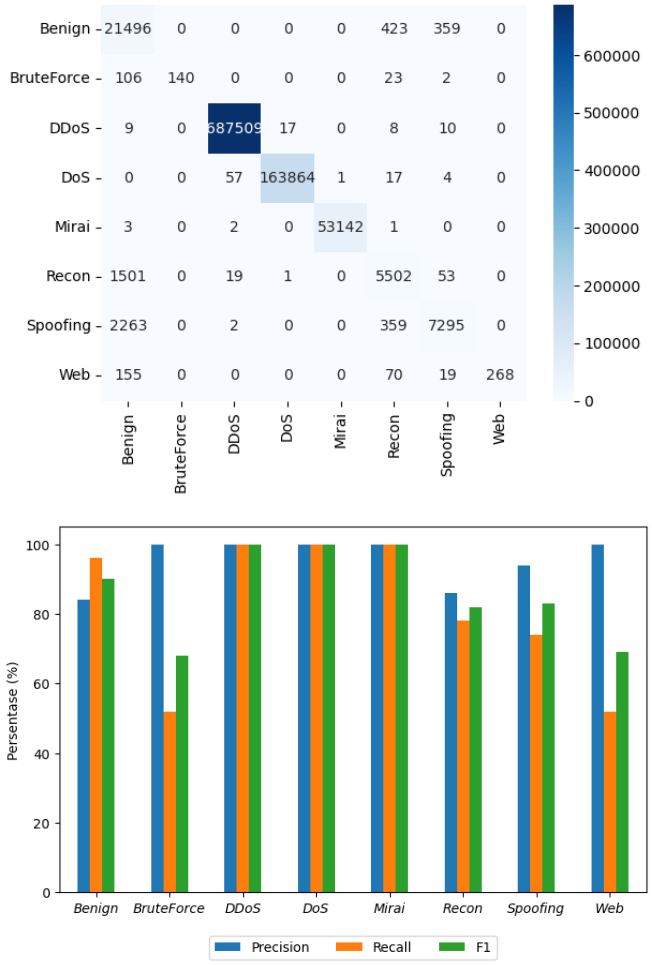
Tahap selanjutnya adalah teknik *feature importance*, yang bertujuan untuk memilih fitur-fitur yang berpengaruh besar terhadap model. Teknik ini dilakukan dengan membangun model DT terlebih dahulu dari 28 fitur terpilih hasil filter korelasi. Kemudian, dilakukan ekstraksi nilai-nilai pada atribut *feature_importance* dan diurutkan seperti ditampilkan pada Gambar 2.

Gambar 2 menunjukkan bahwa terdapat beberapa fitur yang memiliki nilai *feature importance* yang jauh lebih tinggi dari-pada fitur-fitur lainnya. Hal ini menunjukkan bahwa fitur-fitur tersebut memiliki pengaruh yang besar terhadap model. Sebaliknya, beberapa fitur memiliki nilai yang rendah atau bahkan mendekati nol, yang menunjukkan tidak adanya pengaruh yang signifikan terhadap model. Kemudian,

TABEL VI
PERBANDINGAN KINERJA MODEL DETEKSI SERANGAN

Model	Akurasi (%)	Presisi (%)	*Recall* (%)	*F*1 (%)	Waktu Komputasi (s)	Pengurangan Waktu (%)
DT semua fitur	99,56	99,56	99,56	99,56	56,20	-
DT dengan SF	99,37	99,37	99,37	99,37	7,20	87,19
DT dengan SF dan GS	99,64	99,64	99,64	99,64	3,50	93,77
DT dengan SF dan RS	99,64	99,64	99,64	99,64	4,91	91,26
DT dengan SF dan OB	99,64	99,64	99,64	99,64	3,59	93,61
RF semua fitur	99,74	99,74	99,74	99,74	569,60	-
RF dengan SF	99,74	99,74	99,74	99,74	330,40	41,99
RF dengan SF dan GS	99,63	99,63	99,63	99,63	15,49	97,28
RF dengan SF dan RS	99,64	99,64	99,64	99,64	156,33	72,55
RF dengan SF dan OB	99,63	99,64	99,63	99,63	14,73	97,41

SF: seleksi fitur; GS: *grid search*; RS: *random search*; OB: optimasi Bayesian



Gambar 3. Evaluasi kinerja model dengan algoritma *decision tree*.

penelitian ini memilih lima fitur teratas sebagai hasil akhir dari teknik seleksi fitur gabungan dengan penjelasan sebagai berikut.

1. URG_count adalah jumlah paket data dengan *urg flag* dalam satu aliran data yang sama;
2. IAT atau *inter-arrival time* yaitu perbedaan waktu kedatangan antara dua paket data yang berurutan;
3. Variance adalah varians panjang paket data yang masuk dan keluar dalam satu aliran data;
4. Min merupakan minimum panjang paket data dalam satu aliran data yang sama; dan
5. Header_Length ialah panjang *header* yang merupakan bagian awal dari paket data yang berisi informasi kendali untuk pengiriman dan pemrosesan data.

Kemudian, terhadap fitur-fitur hasil seleksi fitur gabungan dilakukan evaluasi perbandingan kinerja dengan beberapa teknik seleksi fitur tunggal menggunakan algoritma DT seperti ditampilkan pada Tabel IV. Tampak bahwa teknik gabungan menghasilkan waktu komputasi yang paling rendah dari semua teknik tunggal, yaitu sebesar 7,20 s, atau pengurangan waktu yang paling tinggi, yaitu sebesar 87,19%. Hal ini menunjukkan bahwa teknik gabungan memiliki keunggulan pada efisiensi penggunaan sumber daya. Meskipun demikian, tingkat akurasinya tidak lebih tinggi dari beberapa teknik tunggal. Hal ini dapat terjadi karena jumlah fitur yang terpilih paling sedikit jika dibandingkan dengan teknik lainnya, sehingga terdapat kemungkinan beberapa fitur penting yang tidak terpilih. Namun, hasil ini telah menunjukkan bahwa terdapat pertimbangan antara efektivitas dengan efisiensi model, yaitu makin banyak jumlah fitur yang digunakan, makin tinggi tingkat akurasi yang dapat dihasilkan oleh model, tetapi makin lama pula waktu komputasi yang dibutuhkan. Sebaliknya, pengurangan fitur dapat mengurangi waktu komputasi, meskipun menurunkan tingkat akurasi. Oleh karena itu, teknik seleksi fitur gabungan perlu digabungkan dengan teknik HPO untuk meningkatkan kembali tingkat akurasinya.

B. DETEKSI SERANGAN DENGAN OPTIMASI BAYESIAN

Model deteksi serangan siber berbasis ML pada penelitian ini dibangun dengan menggunakan algoritma yang tangguh dan ringan pada jaringan IoT, yaitu DT dan RF. Peningkatan kinerja model awal telah dilakukan dengan menurunkan dimensi data menggunakan teknik seleksi fitur gabungan yang memilih lima fitur paling informatif, yaitu URG_count, IAT, Variance, Min, dan Header_Length. Selanjutnya, peningkatan kinerja model dilakukan dengan teknik optimasi Bayesian untuk menemukan nilai optimal dari parameter-parameter algoritma yang digunakan. Teknik ini dilakukan dengan menggunakan pustaka scikit-optimize (skopt) pada ruang pencarian nilai parameter-parameter seperti pada Tabel III. Fungsi objektif yang digunakan untuk optimasi adalah tingkat akurasi dengan jumlah validasi silang sebanyak lima kali. Kemudian, nilai-nilai optimal diekstraksi menggunakan atribut *best_params* seperti yang ditampilkan pada Tabel V.

Tabel V menunjukkan nilai-nilai parameter yang optimal dari teknik optimasi Bayesian untuk algoritma DT dan RF. Pada algoritma DT, nilai parameter *criterion* yang terbaik adalah *gini*, sedangkan pada algoritma RF, nilai parameter *criterion* yang terbaik adalah *entropy*. Di sisi lain, parameter *max_depth*, *min_samples_split*, dan *min_samples_leaf* pada kedua algoritma memiliki nilai-nilai parameter optimal yang sama. Terakhir, jumlah pohon keputusan yang optimal pada

TABEL VII
PERBANDINGAN KINERJA MODEL DENGAN PENELITIAN SEBELUMNYA

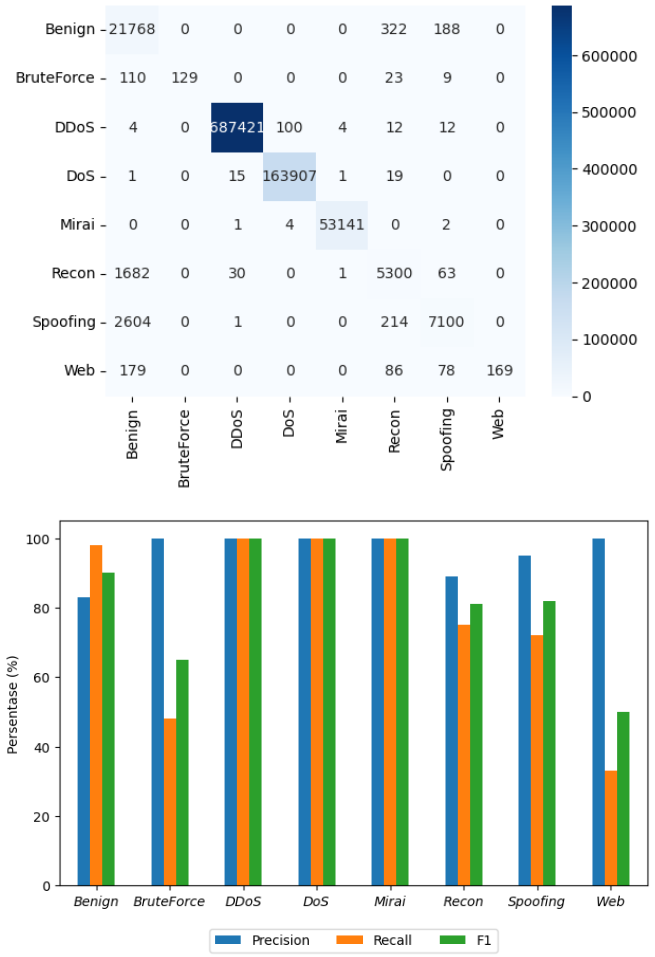
Referensi	Model	Nilai Terbaik
[11]	Model ML: *logistic regression*, *perceptron*, Adaboost, RF, dan DNN	Akurasi: 99,68% Presisi: 96,52% *Recall*: 96,54% *F*1: 96,53%
[12]	Model DL: DNN, CNN, dan LSTM	Akurasi: 99,40% Presisi: 99,43% *Recall*: 99,40% *F*1: 99,41% Waktu komputasi: 625 s
[13]	Model ML gabungan (DT-RF-GB) dengan seleksi fitur *feature importance*	Akurasi: 99,51% Presisi: 98,51% *Recall*: 99,63% *F*1: 99,07% Waktu komputasi: 452 s
[21]	Model DL gabungan (DNN-BiLSTM) dengan seleksi fitur *feature importance* dan HPO Optuna	Akurasi: 93,13% Presisi: 91,80% *Recall*: 93,13% *F*1: 91,94% Waktu komputasi: 714,8 s
Penelitian ini	Model DT dengan seleksi fitur gabungan dan optimasi Bayesian	Akurasi: 99,64% Presisi: 99,64% *Recall*: 99,64% *F*1: 99,64% Waktu komputasi: 3,59 s

algoritma RF adalah sebanyak 28. Kemudian, model dievaluasi dengan perbandingan kinerja antara model tanpa teknik HPO dengan model dengan beberapa teknik HPO, seperti *grid search*, *random search*, dan optimasi Bayesian.

Tabel VI menunjukkan bahwa semua model memiliki kinerja yang tinggi karena memiliki tingkat akurasi, presisi, *recall*, dan *F*1 di atas 99%. Pada algoritma DT, teknik seleksi fitur gabungan dan semua teknik HPO mampu meningkatkan kinerja model dari 99,56% menjadi 99,64% dengan menurunkan waktu komputasi. Teknik HPO dengan GS dan OB mampu menurunkan waktu komputasi model secara signifikan hingga menjadi 3,50 s dan 3,59 s atau 93,77% dan 93,61%. Sementara itu, pada algoritma RF, teknik seleksi gabungan fitur mampu menurunkan waktu komputasi model dari 569,60 s menjadi 330,40 s atau sebesar 41,99%, dengan tetap menjaga tingkat akurasi, presisi, *recall*, dan *F*1 yang tinggi, yaitu 99,74%. Di sisi lain, penggunaan teknik HPO menurunkan tingkat akurasi hingga menjadi 99,63% untuk semua teknik HPO. Meskipun terdapat penurunan tingkat akurasi, teknik HPO mampu menurunkan waktu komputasi model dari 569,60 s menjadi 15,49 s atau 97,28% pada teknik GS, 156,33 s atau 72,55% pada teknik RS, dan 14,73 s atau 97,41% pada teknik OB.

Pada evaluasi kinerja dengan penelitian sebelumnya, Tabel VII menunjukkan bahwa model yang diusulkan menghasilkan tingkat akurasi, presisi, *recall*, dan *F*1 yang paling tinggi, dengan waktu komputasi yang paling rendah. Hal ini menunjukkan bahwa model memiliki keunggulan yang lebih baik dalam hal efektivitas dan efisiensi, sehingga dapat diterapkan pada jaringan IoT. Kemudian, fitur-fitur dan nilai-nilai parameter model yang diperoleh dievaluasi pada model deteksi serangan yang terdiri atas tujuh jenis serangan, seperti yang ditunjukkan pada Gambar 3 dan Gambar 4.

Gambar 3 menampilkan evaluasi kinerja model algoritma DT dengan menggunakan fitur dan parameter hasil proses sebelumnya untuk mendeteksi jenis-jenis serangan yang



Gambar 4. Evaluasi kinerja model dengan algoritma *random forest*.

terdapat pada jaringan IoT. Pada grafik, diketahui bahwa tingkat presisi yang paling tinggi, yaitu 100%, terdapat pada serangan *brute force*, DDoS, DoS, Mirai, dan *web*, yang menunjukkan bahwa model sangat efektif dalam mengidentifikasi serangan-serangan tersebut tanpa ada *false positive*. Hal ini dapat terjadi karena jenis-jenis serangan tersebut memiliki pola data yang unik dan hampir tidak memiliki kemiripan dengan jenis serangan lainnya. Tingkat *recall* yang paling tinggi, yaitu 100%, terdapat pada serangan DDoS, DoS, dan Mirai, yang menunjukkan bahwa model sangat sensitif dalam mengidentifikasi serangan-serangan tersebut tanpa ada *false negative*. Terakhir, nilai *F*1 yang paling tinggi, yaitu 100%, juga terdapat pada serangan DDoS, DoS, dan Mirai, yang menunjukkan bahwa model memiliki keseimbangan yang sempurna dalam mengidentifikasi serangan tersebut. Hasil ini membuktikan bahwa model yang dibangun dengan algoritma DT mampu mendeteksi jenis-jenis serangan siber pada jaringan IoT secara baik.

Gambar 4 menampilkan evaluasi kinerja model algoritma RF dengan menggunakan fitur dan parameter hasil proses sebelumnya untuk mendeteksi jenis-jenis serangan yang terdapat pada jaringan IoT. Pada grafik, diketahui bahwa tingkat presisi yang paling tinggi, yaitu 100%, terdapat pada serangan *brute force*, DDoS, DoS, Mirai, dan *Web*, yang menunjukkan bahwa model sangat efektif dalam mengidentifikasi serangan-serangan tersebut tanpa ada *false positive*. Hal ini dapat terjadi karena jenis-jenis serangan tersebut memiliki pola data yang unik dan hampir tidak memiliki kemiripan dengan jenis serangan lainnya. Sementara

itu, tingkat *recall* yang paling tinggi, yaitu 100%, terdapat pada serangan DDoS, DoS, dan Mirai, yang menunjukkan bahwa model sangat sensitif dalam mengidentifikasi serangan-serangan tersebut tanpa adanya *false negative*. Terakhir, nilai *F*1 yang paling tinggi, yaitu 100%, juga terdapat pada serangan DDoS, DoS, dan Mirai, yang menunjukkan bahwa model memiliki keseimbangan yang sempurna dalam mengidentifikasi serangan tersebut. Hasil ini membuktikan bahwa model yang dibangun dengan algoritma RF mampu mendeteksi jenis-jenis serangan siber pada jaringan IoT secara baik.

V. KESIMPULAN

Model deteksi serangan siber berbasis ML menjadi alternatif terbaik untuk menangani risiko serangan siber pada jaringan IoT yang terus berkembang dengan sangat pesat. Penggunaan seleksi fitur untuk mengurangi dimensi data dan HPO untuk menemukan nilai optimal dari parameter-parameter algoritma ML diperlukan untuk meningkatkan kinerja model. Penelitian ini mengusulkan teknik seleksi fitur gabungan yang menggabungkan filter korelasi dan *feature importance*. Selain itu, teknik optimasi Bayesian juga digunakan untuk menemukan nilai optimal parameter-parameter algoritma ML yang digunakan, yaitu DT dan RF. *Dataset* serangan siber pada jaringan IoT yang terbaru dan tervalidasi, yaitu CICIoT2023, digunakan untuk mengevaluasi model. Hasil penelitian menunjukkan bahwa teknik seleksi fitur gabungan memiliki keunggulan pada waktu komputasinya, yaitu paling rendah dari semua teknik tunggal, yakni sebesar 7,20 s, dan pengurangan waktu yang paling tinggi, yaitu sebesar 87,19%, dengan memilih lima fitur yang paling relevan terhadap model, yaitu URG_count, IAT, Variance, Min, dan Header_Length. Selain itu, kombinasi model dengan teknik HPO menggunakan optimasi Bayesian mampu meningkatkan kinerja model dengan tingkat akurasi 99,64% dan waktu komputasi 3,59 s pada algoritma DT serta tingkat akurasi 99,63% dan waktu komputasi 14,73 s pada algoritma RF. Oleh karena itu, model deteksi serangan siber berbasis ML yang diusulkan dapat menjadi rujukan dalam penerapan keamanan siber pada jaringan IoT.

KONTRIBUSI PENULIS

Konseptualisasi, Samsudiat; metodologi, Samsudiat; perangkat lunak, Samsudiat; validasi, Kalamullah Ramli; analisis formal, Samsudiat; sumber daya, Samsudiat; kurasi data, Samsudiat; penulisan—penyusunan draf asli, Samsudiat; penulisan—peninjauan dan penyuntingan, Samsudiat dan Kalamullah Ramli; visualisasi, Samsudiat; pengawasan, Kalamullah Ramli; administrasi proyek, Samsudiat; akuisisi pendanaan, Samsudiat.

UCAPAN TERIMA KASIH

Penelitian ini mendapatkan dukungan pendanaan dari Program Beasiswa Kementerian Komunikasi dan Digital dan dukungan infrastruktur dari Badan Riset dan Inovasi Nasional.

REFERENSI

[1] I.M.A. Alonso, "IoT cybersecurity: Protecting the merging of the physical and digital world," Telefónica. Tanggal akses: 26-Des-2024. [Online]. Tersedia: https://www.telefonica.com/en/communication-room/blog/iot-cybersecurity-protecting-the-merging-of-the-physical-and-digital-world/

[2] S. Haque, F. El-Moussa, M. Komninos, dan R. Muttukrishnan, "A systematic review of data-driven attack detection trends in IoT," *Sensors,* vol. 23, no. 16, hal. 1–29, Agu. 2023, doi: 10.3390/s23167191.

[3] K. Shafique dkk., "Internet of things (IoT) for next-generation smart systems: A review of current challenges, future trends, and prospects for emerging 5G-IoT scenarios," *IEEE Access*, vol. 8, hal. 23022–23040, Jan. 2020, doi: 10.1109/ACCESS.2020.2970118.

[4] "Lanskap Keamanan Siber Indonesia 2024," Badan Siber dan Sandi Negara, 2025.

[5] R. Mahmoud, T. Yousuf, F. Aloul, dan I. Zualkernan, "Internet of things (IoT) security: Current status, challenges, and prospective measures," dalam *2015 10th Int. Conf. Internet Technol. Secur. Trans. (ICITST)*, 2015, hal. 336–341, doi: 10.1109/ICITST.2015.7412116.

[6] S. Yaras dan M. Dener, "IoT-based intrusion detection system using new hybrid deep learning algorithm," *Electronics,* vol. 13, no. 6, hal. 1–28, Mar. 2024, doi: 10.3390/electronics13061053.

[7] M.A. Al-Garadi dkk., "A survey of machine and deep learning methods for Internet of things (IoT) security," *IEEE Commun. Surv. Tutor.*, vol. 22, no. 3, hal. 1646–1685, Apr. 2020, doi: 10.1109/COMST.2020.2988293.

[8] N. Mishra dan S. Pandya, "Internet of things applications, security challenges, attacks, intrusion detection, and future visions: A systematic review," *IEEE Access*, vol. 9, hal. 59353–59377, Apr. 2021, doi: 10.1109/ACCESS.2021.3073408.

[9] G.T. Reddy dkk., "Analysis of dimensionality reduction techniques on big data," *IEEE Access*, vol. 8, hal. 54776–54788, Mar. 2020, doi: 10.1109/ACCESS.2020.2980942.

[10] P. Sahu dkk., "Enhancing industrial IoT intrusion detection with hyperparameter optimization," dalam *2024 15th Int. Conf. Comput. Commun. Netw. Technol. (ICCCNT)*, 2024, hal. 1–6, doi: 10.1109/ICCCNT61001.2024.10723326.

[11] E.C.P. Neto dkk., "CICIoT2023: A real-time dataset and benchmark for large-scale attacks in IoT environment," *Sensors,* vol. 23, no. 13, hal. 1–26, Jul. 2023, doi: 10.3390/s23135941.

[12] F.L. Becerra-Suarez, V.A. Tuesta-Monteza, H.I. Mejia-Cabrera, dan J. Arcila-Diaz, "Performance evaluation of deep learning models for classifying cybersecurity attacks in IoT networks," *Informatics*, vol. 11, no. 2, hal. 1–13, Jun. 2024, doi: 10.3390/informatics11020032.

[13] T.-T.-H. Le dkk., "Toward enhanced attack detection and explanation in intrusion detection system-based IoT environment data," *IEEE Access*, vol. 11, hal. 131661–131676, Nov. 2023, doi: 10.1109/ACCESS.2023.3336678.

[14] B. Susilo, A. Muis, dan R.F. Sari, "Intelligent intrusion detection system against various attacks based on a hybrid deep learning algorithm," *Sensors*, vol. 25, no. 2, hal. 1–26, Jan. 2025, doi: 10.3390/s25020580.

[15] Q.R.S. Fitni dan K. Ramli, "Implementation of ensemble learning and feature selection for performance improvements in anomaly-based intrusion detection systems," dalam *2020 IEEE Int. Conf. Ind. 4.0 Artif. Intell. Commun. Technol. (IAICT)*, 2020, hal. 118–124, doi: 10.1109/IAICT50021.2020.9172014.

[16] W. Lian dkk., "An intrusion detection method based on decision tree-recursive feature elimination in ensemble learning," *Math. Probl. Eng.*, vol. 2020, no. 1, hal. 1–15, Nov. 2020, doi: 10.1155/2020/2835023.

[17] A.A. Megantara dan T. Ahmad, "Feature importance ranking for increasing performance of intrusion detection system," dalam *2020 3rd Int. Conf. Comput. Inform. Eng. (IC2IE)*, 2020, hal. 37–42, doi: 10.1109/IC2IE50715.2020.9274570.

[18] H. Kurniawan dkk., "Enhancing the detection of botnet attacks in the Internet of things networks through the utilization of hybrid feature selection," dalam *2024 FORTEI-Int. Conf. Electr. Eng. (FORTEI-ICEE)*, 2024, hal. 89–94, doi: 10.1109/FORTEI-ICEE64706.2024.10824638.

[19] J.J. Shirley dan M. Priya, "Hybrid MRMR-PCA BagDT – An effective feature selection based ensemble model for real-time intrusion detection in IoT environment," *IEEE Access*, vol. 12, hal. 144230–144248, Sep. 2024, doi: 10.1109/ACCESS.2024.3468897.

[20] J.-B. Altidor dan C. Talhi, "Enhancing port scan and DDoS attack detection using genetic and machine learning algorithms," dalam *2024 7th Conf. Cloud Internet Things (CIoT)*, 2024, hal. 1–7, doi: 10.1109/CioT63799.2024.10757005.

[21] Y.N. Kunang, S. Nurmaini, D. Stiawan, dan B.Y. Suprapto, "Improving classification attacks in IoT intrusion detection system using Bayesian hyperparameter optimization," dalam *2020 3rd Int. Semin. Res. Inf. Technol. Intell. Syst. (ISRITI)*, 2020, hal. 146–151, doi: 10.1109/ISRITI51436.2020.9315360.

[22] K. Ashton, "That 'Internet of things' thing." RFID JOURNAL. Tanggal akses: 26-Des-2024. [Online]. Tersedia: https://www.rfidjournal.com/expert-views/that-internet-of-things-thing/73881

[23] L. Chettri dan R. Bera, "A comprehensive survey on Internet of things (IoT) toward 5G wireless systems," *IEEE Internet Things J.*, vol. 7, no. 1, hal. 16–32, Jan. 2020, doi: 10.1109/JIOT.2019.2948888.

[24] S. Dange dan M. Chatterjee, "IoT botnet: The largest threat to the IoT network," dalam *Data Commun. Netw., Proc. GUCON 2019*, 2019, hal. 137–157, doi: 10.1007/978-981-15-0132-6_10.

[25] S. Yamaguchi, "Botnet defense system: Concept, design, and basic strategy," *Information*, vol. 11, no. 11, hal. 1–15, Nov. 2020, doi: 10.3390/info11110516.

[26] Y. Lu dan L.D. Xu, "Internet of things (IoT) cybersecurity research: A review of current research topics," *IEEE Internet Things J.*, vol. 6, no. 2, hal. 2103–2115, Apr. 2019, doi: 10.1109/JIOT.2018.2869847.

[27] Y. Xin dkk., "Machine learning and deep learning methods for cybersecurity," *IEEE Access*, vol. 6, hal. 35365–35381, Mei 2018, doi: 10.1109/ACCESS.2018.2836950.

[28] H.-J. Liao, C.-H.R. Lin, Y.-C. Lin, dan K.-Y. Tung, "Intrusion detection system: A comprehensive review," *J. Netw. Comput. Appl.*, vol. 36, no. 1, hal. 16-24, Jan. 2013, doi: 10.1016/j.jnca.2012.09.004.

[29] F. Hussain, R. Hussain, S.A. Hassan, dan E. Hossain, "Machine learning in IoT security: Current solutions and future challenges", *IEEE Commun. Surv. Tutor.,* vol. 22, no. 3, hal. 1686–1721, Apr. 2020, doi: 10.1109/COMST.2020.2986444.

[30] L. Breiman, J. Friedman, R.A. Olshen, dan C.J. Stone, *Classification and Regression Trees.* New York, NY, AS: Chapman & Hall/CRC, 2017.

[31] B. Mahbooba, M. Timilsina, R. Sahal, dan M. Serrano, "Explainable artificial intelligence (XAI) to enhance trust management in intrusion detection systems using decision tree model," *Complexity,* vol. 2021, no. 1, hal. 1–11, Jan. 2021, doi: 10.1155/2021/6634811.

[32] L. Breiman, "Random forests," *Mach. Learn.*, vol. 45, hal. 5-32, Okt. 2001, doi: 10.1023/A:1010933404324.

[33] A.K. Balyan dkk., "A hybrid intrusion detection model using EGA-PSO and improved random forest method," *Sensors,* vol. 22, no. 16, hal. 1–20, Agu. 2022, doi: 10.3390/s22165986.

[34] Canadian Institute for Cybersecurity (CIC), 2023, "CIC IoT Dataset 2023", Canadian Institute for Cybersecurity (CIC), University of New Brunswick (UNB), Kanada. [Online]. Tersedia: https://www.unb.ca/cic/datasets/iotdataset-2023.html

[35] I. Guyon dan A. Elisseeff, "An introduction to variable and feature selection," *J. Mach. Learn. Res.*, vol. 3, hal. 1157-1182, Mar. 2003, doi: 10.1162/153244303322753616.

[36] D. Edelmann, T.F. Móri, dan G.J. Székely, "On relationships between the Pearson and the distance correlation coefficients," *Stat. Probab. Lett.*, vol. 169, hal. 1–6, Feb. 2021, doi: 10.1016/j.spl.2020.108960.

[37] I.H. Sarker, Y.B. Abushark, F. Alsolami, dan A.I. Khan, "IntruDTree: A machine learning based cyber security intrusion detection model," *Symmetry,* vol. 12, no. 5, hal. 1–15, Mei 2020, doi: 10.3390/sym12050754.

[38] B. Bischl dkk., "Hyperparameter optimization: Foundations, algorithms, best practices, and open challenges," *WIREs Data Min. Knowl. Discov.*, vol. 13, no. 2, hal. 1–43, Mar./Apr. 2023, doi: 10.1002/widm.1484.

[39] R. Zuech, J. Hancock, dan T.M. Khoshgoftaar, "Detecting web attacks using random undersampling and ensemble learners," *J. Big Data*, vol. 8, no. 1, hal. 1–20, Mei 2021, doi: 10.1186/s4053-021-00460-8.

[40] M.A. Umar, Z. Chen, K. Shuaib, dan Y. Liu, "Effects of feature selection and normalization on network intrusion detection," *Data Sci. Manag.*, vol. 8, no. 1, hal. 23-39, Mar. 2025, doi: 10.1016/j.dsm.2024.08.001.