MEAN ABSOLUTE DIFFERENCE (MAD) SEBAGAI METODE PEMILIHAN FITUR U DETEKSI SERANGAN PADA JARINGAN *INT OF MEDICAL THINGS* MENGGUNAKAN AL TMA *RANDOM FOREST* DAN *GRADIENT BOOSTING*

UNIVERSITAS BINA INSAN

SKRIPSI

Diajukan Sebagai Syarat Untuk Menyelesaikan Pendidikan

Program Sarjana (S-1)

Pada Program Studi Rekayasa Sistem Komputer

Oleh :
MERYANDI ANDIKA PUTRA
NIM : 2102010030

PROGRAM STUDI REKAYASA SISTEM KOMPUTER
FAKULTAS ILMU TEKNIK
UNIVERSITAS BINA INSAN
2024/2025

HALAMAN PENGESAHAN SKRIPSI

MEAN ABSOLUTE DIFFERENCE (MAD) SEBAGAI METODE PEMILIHAN FITUR UNTUK DETEKSI SERANGAN PADA JARINGAN *INTERNET OF MEDICAL THINGS* MENGGUNAKAN ALGORITMA *RANDOM FOREST* DAN *GRADIENT BOOSTING*

Oleh :
MERYANDI ANDIKA PUTRA
NIM : 2102010030

Lubuklinggau, 24 Januari 2025

Pembimbing I	**Pembimbing II**
(Dr. M. Agus Syamsul Arifin, S.St., M.Kom)	**(Bunga Intan, M.Kom)**

Mengetahui,
Dekan Fakultas Ilmu Teknik
Universitas Bina Insan

(Dr. Rudi Kurniawan, ST., M.Kom)

HALAMAN PERSETUJUAN TIM PENGUJI SKRIPSI

Pada hari Jum‘at tanggal 24 bulan Januari tahun 2025 telah dilaksanakan sidang Skripsi oleh Program Studi Rekayasa Sistem Komputer Universitas Bina Insan.

Nama : Meryandi Andika Putra
NIM : 2102.01.0030
Judul Skripsi : *Mean Absolute Difference (MAD)* sebagai metode pemilihan fitur untuk deteksi serangan pada jaringan *Internet of Medical Things* menggunakan algoritma *Random Forest* dan *Gradient Boosting*

Komisi Penguji

1. Ketua : Dr. M. Agus Syamsul Arifin, S.St., M.Kom ( )

2. Sekretaris : Bunga Intan, M.Kom ( )

3. Anggota : Novi Lestari, M.Kom ( )

Mengetahui,
Kepala Program Studi Rekayasa Sistem Komputer
Universitas Bina Insan

(Armanto, M.Kom)

HALAMAN MOTTO DAN PERSEMBAHAN

MOTTO

- KUNCI KESUKSESAN DALAM [illegible] WISUDA IYALAH DUIT (DOA, USAHA, IKTIAR DAN TAWAKAL).
- SETIAP ORANG MEMILIKI PROSES BERBEDA-BEDA DALAM MENGGAPAI KESUKSESAN, SEMAKIN SULIT PROSES YANG KAMU HADAPI SEMAKIN BESAR PULA KESUKSESAN YANG KAMU DAPATI.
- KAMU BOLEH TERLAHIR DARI KELUARGA YANG KURANG MAMPU, TAPI KAMU TIDAK BOLEH MENERUSKANNYA UNTUK GENERASIMU DIMASA DEPAN, JADIKAN DIRIMU SEBAGAI PEMUTUS TALI KEMISKINAN DALAM KELUARGA MU DAN JADIKAN ORANG TUAMU BANGGA ATAS KESUKSESANMU DIMASA DEPAN.
- MATER EST FONS VITAE (IBU ADALAH SUMBER KEHIDUPAN)

PERSEMBAHAN KEPADA :

- *ALLAH SWT YANG TELAH MEMBERIKAN RAHMAT DAN HIDAYAHNYA.*
- *IBU YANG SELALU SUPPORT DAN MENDOAKANKU.*
- *TEMAN-TEMAN YANG SELALU SUPPORT MEMBANTUKU.*
- *TERIMA KASIH CHATGPT TELAH MEMBANTU DALAM PENELITIAN INI*

HALAMAN PERNYATAAN

Saya yang bertand[illegible] dibawah ini :

Nama : Meryandi Andika Putra

Nim : 2102010030

Program Studi : Rekayasa Sistem Komputer

Menyatakan dengan sesunggunya bahwa penelitian dan penulisan skripsi yang saya susun sebagai persyaratan untuk memperoleh gelar sarjana (S-1) Universitas Bina Insan, merupakan hasil kerja saya sendiri dan tidak menyuruh orang lain yang mengerjakannya. Ada bagian tertentu dalam penulisan skripsi ini yang saya kutip dari hasil karya orang lain dan telah saya tuliskan sumbernya secara jelas sesuai dengan norma, kaidah dan etika dalam penulisan ilmiah.

Jika dikemudian hari ternyata terbukti bahwa penelitian dan tugas akhir ini bukan hasil kerja saya sendiri atau pla giat dalam bagian tertentu, maka saya bersediah dikenakan sanksi sesuai dengan peraturan perundangan yang berlaku.

Lubuklinggau, 24 Januari 2025

Meryandi Andika Putra

ABSTRACT

The security of the Internet of [illegible]hings (IoMT) network poses a significant challenge due to the increasing [illegible] cyberattacks. This study aims to improve the accuracy of attack detection using the Mean Absolute Difference (MAD) method for feature selection and the Random Forest and Gradient Boosting algorithms for classification. The data were validated using the 10-fold cross-validation technique. The results show that the Random Forest algorithm with MAD-based feature selection achieved an accuracy of up to 100%, while Gradient Boosting also demonstrated high performance, albeit slightly lower. This study proves the effectiveness of MAD in enhancing the performance of attack detection models. The implication of this research is the development of more efficient and accurate IoMT network security systems in the future.

Kata Kunci: *Mean Absolute Difference, Random Forest, Gradient Boosting, Internet of Medical Things, Intrusion Detection System.*

ABSTRAK

Keamanan jaringan *Internet of* [illegible] *Things (IoMT)* menjadi tantangan besar akibat tingginya ancaman s[illegible] siber. Penelitian ini bertujuan untuk meningkatkan akurasi deteksi serangan dengan menggunakan metode *Mean Absolute Difference (MAD)* untuk seleksi fitur, serta algoritma *Random Forest* dan *Gradient Boosting* untuk klasifikasi. Data yang digunakan divalidasi menggunakan teknik 10-*fold cross-validation*. Hasil penelitian menunjukkan bahwa algoritma *Random Forest* dengan seleksi fitur MAD mencapai akurasi hingga 100%, sementara *Gradient Boosting* juga menunjukkan performa tinggi meskipun sedikit lebih rendah. Penelitian ini membuktikan efektivitas MAD dalam meningkatkan performa model deteksi serangan. Implikasi dari penelitian ini adalah pengembangan sistem keamanan jaringan IoMT yang lebih efisien dan akurat di masa mendatang.

Kata Kunci: *Mean Absolute Difference, Random Forest, Gradient Boosting, Internet of Medical Things, Intrusion Detection System.*

KATA PENGANTAR

Alhamdulillah puji dan [illegible]nulis panjatkan kepada Allah SWT yang telah melimpahkan segala ra[illegible] hidayah-Nya, sehingga penulis dapat menyelesaikan skripsi dengan maksimal. Skripsi ini dibuat bertujuan sebagai syarat untuk menyelesaikan pendidikan program sarjana (S-1) pada Program Studi Rekayasa Sistem Komputer Fakultas Ilmu Teknik Universitas Bina Insan Lubuklinggau. Sholawat serta salam semoga tercurahkan kepada Nabi Muhammad SAW, keluarga, sahabat, serta pengikutnya hingga akhir zaman.

Dalam penulisan skripsi ini penulis telah berusaha untuk menyajikan sebaik mungkin, baik dari segi penulisan dan dari segi desain. Penulis menyadari bahwa dalam hal penulisan ini tentunya masih jauh dari kata sempurna, hal ini dikarenakan keterbatasan pengetahuan yang dimiliki. Oleh karena itu dalam rangka melengkapi kesempurnaan dari penulisan skripsi ini diharapkan adanya kritik dan saran yang bersifat membangun.

Pada kesempatan ini penulis mengucapkan terima kasih yang sebesar-besarnya kepada :

1. Bapak Dr. H. Sardiyo, M.M selaku Rektor Universitas Bina Insan Lubuklinggau.
2. Bapak M. Akbar, S.T, M.IT Selaku Wakil Rektor I Universitas Bina Insan Lubuklinggau.
3. Bapak Wakhid Nur Mukhlis, M.Pd selaku Wakil Rektor II Universitas Bina Insan Lubuklinggau.
4. Bapak Dr. Rudi Kurniawan, S.T, M.Kom Selaku Dekan Fakultas Ilmu Teknik Universitas Bina Insan Lubuklinggau.
5. Bapak Armanto, M.Kom Selaku Ketua Program Studi Rekayasa Sistem Komputer yang telah banyak memberikan arahan dan bimbingan dalam penulisan Skripsi ini.

6. Bapak Dr. M. Agus Syamsul Arifin, S.St., M.Kom Selaku pembimbing I yang telah banyak mem[illegible] arahan dan bimbingan dalam penyelesaian Skripsi ini.
7. Ibu Bunga Intan, M.K[illegible]ku pembimbing II yang telah banyak memberikan arahan dan bimbingan dalam penyelesaian Skripsi ini.
8. Seluruh Staf Dosen dan Karyawan Universitas Bina Insan Lubuklinggau yang telah banyak memberikan ilmu pengetahuan dan bimbingan kepada penulis.
9. Ibuku yang telah memberikan Support & doa sehingga bersemangat agar dapat menyelesaikan skripsi ini.
10. Teman-teman seperjuangan dan sejawat saya selama menjadi mahasiswa prodi rekayasa sistem komputer.

Akhir kata semoga penelitian ini dapat bermanfaat untuk penelitian selanjutnya.

Lubuklinggau, 24 Januari 2025

Meryandi Andika Putra
(2102010030)

DAFTAR RIWAYAT HIDUP

Biodata :

Nama	: Meryandi Andika Putra
Tempat/Tanggal Lahir	: Lampung Barat, 18 Agustus 2003
Jenis Kelamin	: Laki-Laki
Status	: Mahasiswa
Agama	: Islam
Alamat	: Jogoboyo Kecamatan Lubuklinggau Utara II, Kota Lubuklinggau.

Pendidikan :

- SD NEGERI 2 Tanjung Ratu Lampung Tengah
- SMP Muhammadiyah Lubuklinggau
- SMK NEGERI 1 Lubuklinggau

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

DAFTAR LAMPIRAN

BAB 1

PENDAHULUAN

1.1 Latar Belakang

Internet of Medical Things (IoMT) adalah jaringan perangkat medis yang terhubung melalui internet, yang merevolusi konsep *Internet of Things (IoT).* Istilah IoT pertama kali diperkenalkan oleh Kevin Ashton pada tahun 1999 di *Massachusetts Institute of Technology (MIT)*. Meskipun konsep IoT terus berkembang pesat, penerapannya secara khusus dalam bidang medis baru dimulai pada tahun 2000-an, seiring dengan kemajuan teknologi sensor dan komunikasi nirkabel. IoMT memungkinkan pemantauan kondisi pasien secara *real-time* melalui perangkat seperti sensor yang memantau tanda-tanda vital pasien dan mengirimkan data secara langsung kepada dokter melalui jaringan internet. Aplikasi ini meningkatkan efisiensi perawatan medis dan memberikan solusi untuk pemantauan pasien jarak jauh [1].

Pada tahun 2020, perhatian utama dalam pengembangan IoMT bergeser ke arah pemanfaatan Kecerdasan Buatan *(Artificial Intelligence/AI)*. Teknologi AI digunakan untuk menganalisis data medis, memberikan prediksi yang lebih akurat terkait diagnosis, serta mengembangkan perawatan yang dipersonalisasi untuk kebutuhan individu pasien. Pendekatan ini bertujuan untuk meningkatkan efisiensi dan efektivitas pada layanan kesehatan yang disediakan melalui IoMT [2]. Pada akhir tahun 2020, IoMT menyumbang 40% dari pasar IoT. Diperkirakan bahwa ini akan terus tumbuh selama beberapa tahun ke depan karena potensi kontribusi IoMT dalam menurunkan biaya disektor kesehatan. Industri ini dapat menghemat hingga $300 miliar dengan lebih mengandalkan perangkat IoMT, terutama untuk pasien penyakit kronis [3].

Meningkatkan kerja sama antara produsen, penyedia layanan kesehatan, dan ahli keamanan siber sangat penting untuk mengembangkan sistem IoMT yang kuat dan aman yang memprioritaskan privasi pasien [4].

Namun, perkembangan cepat IoMT telah berarti bahwa keamanan dan privasi dari sistem kesehata[illegible]sis IoMT ini sering kali kurang mendapat perhatian yang cukup. Kons[illegible]ari keamanan yang tidak memadai dalam sistem kesehatan berbasis I[illegible]t berupa, misalnya, privasi pasien yang terganggu akibat penyadapan, dan keterlambatan deteksi episode yang mengancam jiwa akibat gangguan operasi normal perangkat IoMT yang disebabkan oleh serangan *Denial of Service (DoS)* [5]. Dengan meningkatnya konektivitas, serangan siber pada jaringan IoMT menjadi semakin umum. Salah satu sumber data yang digunakan untuk menganalisis ancaman dilingkungan IoMT adalah CICIoMT2024. Dataset ini dirancang khusus untuk menganalisis dan mendeteksi serangan siber dalam konteks IoMT, termasuk informasi mengenai berbagai jenis serangan yang dapat terjadi pada perangkat medis yang terhubung, seperti DDoS dan *malware*. Selain itu, CICIoMT2024 juga menyediakan karakteristik lalu lintas jaringan yang penting untuk membangun model deteksi serangan yang lebih efektif dan akurat [6].

Untuk mengatasi tantangan ini, penelitian ini akan memanfaatkan dataset CICIoMT2024, yang mencakup skenario serangan pada perangkat IoMT, seperti *Denial-of-Service (DoS), Distributed Denial-of-Service (DDoS),* dan *Man-in-the-Middle (MitM).* Data *test* berjumlah 1,614,182 data (18%), sedangkan data *train* berjumlah 7,160,831 data (82%). Jumlah data keseluruhan *train* dan *test* adalah 8,775,013 data. Dengan menganalisis dataset tersebut, penelitian ini bertujuan untuk pembangunan dan evaluasi model, tanpa implementasi langsung pada sistem nyata. melalui penerapan algoritma *Random Forest* dan *Gradient Boosting*. Selain itu juga, pendekatan *Mean Absolute Difference (MAD)* akan digunakan untuk pemilihan fitur yang relevan. Pendekatan ini diharapkan mampu menghasilkan solusi keamanan IoMT yang akurat.

Dengan ini, penulis akan membuat penelitian proposal dengan judul *Mean Absolute Difference (MAD)* [illegible]ai metode Pemilihan Fitur untuk deteksi serangan pada Jaringan *Int*[illegible]*edical Things* menggunakan algoritma *Random Forest* dan *Gradien*[illegible].

1.2 Identifikasi Masalah

Meningkatnya ancaman keamanan pada jaringan *Internet of Medical Things (IoMT)* menjadi masalah utama dalam penelitian ini. Serangan siber seperti *Denial-of-Service (DoS)* dan *Distributed Denial-of-Service (DDoS)* adalah contoh serangan siber yang dapat membahayakan data pasien dan operasi perangkat medis. Untuk meningkatkan akurasi dan efisiensi algoritma *Machine learning*, seperti *Random Forest* dan *Gradient Boosting*, dalam mendeteksi serangan pada jaringan IoMT, diperlukan pengembangan metode pemilihan fitur yang relevan, seperti *Mean Absolute Difference (MAD)*.

1.3 Rumusan Masalah

Dari hasil identifikasi masalah diatas, maka dapat dirumuskan suatu permasalahan yang akan di jawab dalam penelitian ini adalah **"Bagaimana menerapkan *Mean Absolute Difference (MAD)* sebagai metode pemilihan fitur yang efektif untuk meningkatkan akurasi deteksi serangan pada jaringan *Internet of Medical Things (IoMT)* dengan menggunakan algoritma *Random Forest* dan *Gradient Boosting*?"**

1.4 Batasan Masalah

Penulis menetapkan beberapa batasan masalah dalam penelitian ini, yaitu:

a. Dataset yang digunakan yaitu; CICIoMT2024, yang mencakup berbagai jenis serangan pada jaringan IoMT.

b. Penelitian ini dilakukan menggunakan bahasa pemrograman *Python* dan pustaka pembelajaran mesin seperti *SciKit-learn* akan digunakan untuk pemrograman dan analisis data, serta pustaka standar seperti *Pandas* dan *NumPy*.

c. Penelitian ini berfokus [illegible] mbangunan dan evaluasi model, tanpa implementasi langsung [illegible] m nyata.

1.5 Tujuan dan Manfaat Penelitian

1.5.1 Tujuan Penelitian

Adapun tujuan dari penelitian ini sebagai berikut:

a. Menentukan fitur-fitur yang paling penting untuk mendeteksi serangan dilakukan dengan menerapkan metode *Mean Absolute Difference (MAD).*

b. Mengevaluasi efektivitas algoritma *Random Forest* dan *Gradient Boosting* dalam mendeteksi serangan pada jaringan *Internet of Medical Things (IoMT).*

1.5.2 Manfaat Penelitian

Adapun manfaat Dari penelitian ini sebagai berikut:

a. Memberikan kontribusi terhadap literatur tentang keamanan jaringan IoMT, terutama dengan menerapkan metode MAD untuk pemilihan fitur dan *Gradient Boosting* dan algoritma *Random Forest.*

b. Memberi jaringan IoMT perlindungan yang lebih baik dari serangan, meningkatkan kepercayaan dalam penerapan perangkat IoMT di sektor kesehatan.

c. Meningkatkan keamanan jaringan IoMT terhadap serangan siber, yang memastikan keamanan data pasien dan kelangsungan operasional perangkat medis.

1.6 Sistematika Penulisan

a. Bab I Pendahuluan

Bab ini menjelaskan latar belakang penelitian, identifikasi masalah, rumusan masalah, batasan masalah, tujuan dan manfaat penelitian, serta sistematika penulisan skripsi ini.

b. Bab II Kajian Pustaka

Bab ini memuat litera[illegible] penelitian terdahulu yang relevan, serta kerangka berpikir yang [illegible] acuan dalam analisis dan implementasi penelitian.

c. Bab III Metodologi Penelitian

Bab ini menjelaskan metode penelitian yang digunakan, pengumpulan dan pengolahan data, metode analisis, alat dan bahan, serta tahapan pelaksanaan penelitian.

d. Bab IV Hasil Penelitian dan Pembahasan

Bab ini berisi gambaran umum, hasil penelitian, dan pembahasan mendalam tentang hasil yang diperoleh berdasarkan tujuan penelitian dan analisis data.

e. Bab V Kesimpulan dan Saran

Bab ini menyajikan kesimpulan dari hasil penelitian dan memberikan saran yang bermanfaat untuk penelitian lanjutan atau aplikasi praktis.

f. Daftar Pustaka

Bagian ini berisi sumber referensi yang digunakan dalam penulisan skripsi, meliputi jurnal, buku, dan dokumen lain yang relevan.

g. Lampiran

Bagian lampiran berisi data tambahan, tabel, grafik, atau dokumen pendukung lain yang relevan dengan penelitian.

BAB II

KA[illegible] PUSTAKA

2.1 Literatur

2.1.1 *Intrusion Detection System*

Intrusion Detection System (IDS) adalah sistem yang dilengkapi dengan agen pengumpul data audit untuk memantau aktivitas pada jaringan atau sistem tertentu. Data yang dikumpulkan dapat disimpan atau diproses langsung oleh unit deteksi untuk mengidentifikasi potensi ancaman atau aktivitas mencurigakan. Setelah itu, hasil deteksi ini akan diteruskan ke *Site Security Office (SSO)* untuk ditindaklanjuti. Proses ini biasanya melibatkan langkah tambahan, seperti investigasi lebih lanjut untuk menentukan penyebab alarm yang terdeteksi. [7].

2.1.2 *Feature Selection*

Feature Selection adalah proses memilih subset variabel yang relevan (fitur) untuk digunakan dalam membangun model. Langkah ini sangat penting dalam persiapan data, terutama saat bekerja dengan dataset berdimensi tinggi, di mana banyak variabel mungkin tidak relevan atau redundan. [8]. Dataset sering kali mengandung banyak fitur, namun tidak semuanya memberikan kontribusi signifikan terhadap tugas klasifikasi atau prediksi. Dengan melakukan seleksi fitur, model dapat menghindari kebisingan yang disebabkan oleh data yang tidak relevan, mengurangi risiko *overfitting,* dan hanya memilih fitur yang benar-benar penting bagi performa model [9].

2.1.3 *Mean Absolute Difference*

Mean Absolute Difference (MAD) adalah ukuran statistik yang menghitung rata-rata perbedaan absolut antara nilai dalam dataset, seperti rata-rata atau median [10]. MAD dalam penelitian ini berfungsi sebagai metode pemilihan fitur untuk menemukan fitur yang berkontribusi besar terhadap deteksi serangan pada jaringan IoMT.

$$= \frac{1}{n}\sum_{i=1}^{n}|x_i - \bar{x}|$$

Gambar 2. 1 Formula MAD

Dimana:

x_i adalah nilai individu dalam dataset,

$\bar{x}$ adalah nilai rata-rata dari seluruh data,

n adalah jumlah total data dalam dataset.

2.1.4 *Random Forest*

Random forest adalah metode pembelajaran *ensembel* yang digunakan untuk *klasifikasi* dan *regresi. Random forest* memiliki beberapa keunggulan, seperti jumlah parameter kontrol yang rendah, tahan terhadap *overfitting*. Namun, metode ini juga memiliki beberapa kelemahan, seperti *interpretabilitas* model yang rendah, penurunan kinerja akibat *variabel* terkait, dan ketergantungan pada *generator* acak selama *implementasi* [11].

2.1.5 *Gradient Boosting*

Gradient Boosting adalah algoritma pembelajaran mesin berbasis *ensemble* yang menggabungkan prediksi dari beberapa model sederhana (*weak learners*), seperti pohon keputusan kecil, untuk membentuk model prediksi yang lebih kuat (*strong learners*). Algoritma ini bekerja secara iteratif dengan mengoptimalkan fungsi kerugian (*loss function*) menggunakan pendekatan *gradient descent*. Setiap model baru yang ditambahkan bertujuan untuk mengurangi kesalahan yang dibuat oleh model sebelumnya, sehingga menghasilkan prediksi akhir [illegible] bih akurat [12].

2.1.6 Internet

Internet *(Inter-Network)* merujuk pada jaringan komputer yang saling terhubung, mencakup situs-situs dari berbagai sektor seperti akademik, pemerintahan, komersial, organisasi, serta individu. Internet menyediakan akses kepada layanan telekomunikasi dan sumber daya informasi yang dapat diakses oleh jutaan penggunanya yang tersebar di seluruh dunia. Internet pertama kali dikembangkan pada 1960-an sebagai sarana untuk berbagi informasi antar peneliti, terutama dalam lingkup militer dan akademik [13].

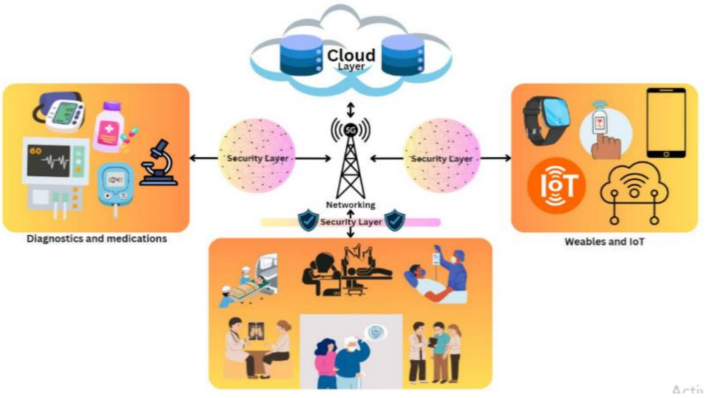
2.1.7 *Internet of Things*

Internet of Things (IoT) merujuk pada jaringan perangkat fisik yang terhubung ke internet, Teknologi ini memungkinkan otomatisasi dan pengolahan data secara *real-time*, yang mempermudah komunikasi antar perangkat di berbagai sektor kehidupan. Konsep *Internet of Things (IoT)* pertama kali diperkenalkan pada tahun 1982 melalui perangkat yang dikenal sebagai *"Coca-Cola Machine"* Perangkat ini, dirancang oleh David Nichols dari *Carnegie Mellon University*, dihubungkan ke internet untuk memantau stok minuman di dalam mesin. Teknologi ini memungkinkan pemilik mesin untuk menerima laporan ketersediaan minuman secara online tanpa perlu melakukan pemeriksaan langsung, menjadi salah satu contoh awal penerapan IoT [14].

Gambar 2. 2 *Internet of Things (IoT)*

2.1.8 *Internet of Medical Things*

Internet of Medical Things (IoMT) merupakan perkembangan dari konsep *Internet of Things (IoT)* yang khusus diterapkan di bidang medis. Perangkat IoMT meliputi berbagai teknologi, seperti alat pemantau kesehatan yang dapat dipakai (*wearable*), alat pacu jantung yang terhubung ke jaringan, hingga perangkat medis yang terintegrasi dengan fasilitas rumah sakit untuk meningkatkan efisiensi dan pemantauan kesehatan pasien [15]. Karena mengelola data yang sensitif, keamanan IoMT menjadi hal yang penting [16].



Gambar 2. 3 *Internet of Medical Things*

Sumber: Mukhopadhyay et al. 2024

2.1.9 *Python*

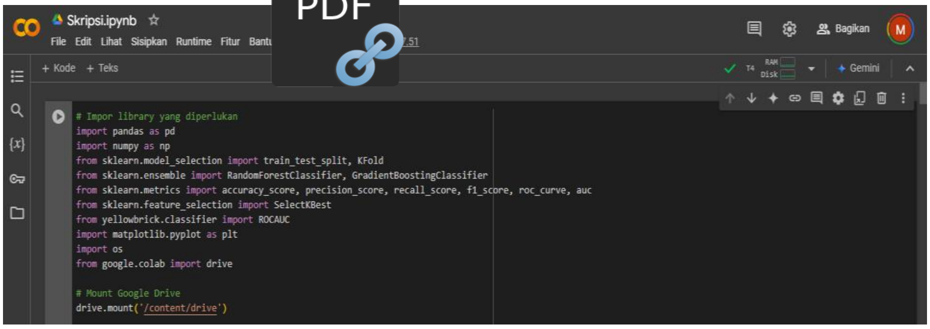
Python adalah bahasa [illegible]raman yang sangat populer dan mudah dipelajari, terutama bagi pe[illegible]h satu alasan utama penggunaan *Python* yang luas adalah sintaksnya yang [illegible]erhana dan jelas, sehingga memudahkan pembaca untuk memahami kode yang ditulis [17]. *Python* juga mendukung berbagai platform, artinya bisa dijalankan di berbagai sistem operasi seperti *Windows, macOS,* dan *Linux.* Berkat *fleksibilitas* dan kemudahan penggunaannya, *Python* menjadi pilihan yang sangat tepat bagi mereka yang ingin belajar pemrograman atau berkarir di bidang teknologi [15].

Python banyak digunakan di berbagai bidang, seperti pengembangan web, analisis data, dan kecerdasan buatan. Salah satu alasan mengapa *Python* begitu populer adalah karena ketersediaan banyak pustaka *(library)* dan *framework* yang mendukung beragam kebutuhan, seperti *NumPy* dan *Pandas* untuk analisis data, serta *TensorFlow* dan *scikit-learn* untuk pembelajaran mesin [6].

Gambar 2. 4 *Python*

2.1.10 Google Colab

Google Colab, yang juga dikenal sebagai Google Colaboratory, adalah platform berbasis *cloud* yang memungkinkan pengguna untuk menulis dan menjalankan kode *Python* dalam bentuk *notebook interaktif.* Platform ini dikembangkan oleh Google untuk membantu para programmer, peneliti, dan ilmuwan data dalam mengembangkan analisis data dan model pembelajaran mesin tanpa perlu menginstal perangkat lunak tambahan. Google Colab memungkinkan pemrosesan gambar dan analisis data besar secara mudah, didukung oleh kekuatan GPU [illegible]PU [18].



```
# Impor library yang diperlukan
import pandas as pd
import numpy as np
from sklearn.model_selection import train_test_split, KFold
from sklearn.ensemble import RandomForestClassifier, GradientBoostingClassifier
from sklearn.metrics import accuracy_score, precision_score, recall_score, f1_score, roc_curve, auc
from sklearn.feature_selection import SelectKBest
from yellowbrick.classifier import ROCAUC
import matplotlib.pyplot as plt
import os
from google.colab import drive

# Mount Google Drive
drive.mount('/content/drive')
```

Gambar 2. 5 Google Collab

2.1.11 Dataset

Dataset merupakan sebuah sekumpulan data yang berasal dari informasi-informasi pada masa lalu dan siap untuk dikelola menjadi sebuah informasi baru[19].

2.1.12 Dataset CICIoMT2024

Dataset CICIoMT2024 dikembangkan oleh *Canadian Institute for Cybersecurity* untuk mendukung penelitian mengenai keamanan siber dalam konteks *Internet of Medical Things (IoMT)*. Dataset ini mencakup data yang telah dilabeli untuk 19 jenis serangan siber, termasuk serangan *Distributed Denial of Service (DDoS)* dan jenis serangan lainnya. Dataset ini sangat berguna untuk menguji algoritma pembelajaran mesin yang bertujuan meningkatkan keamanan IoMT, serta dapat digunakan untuk mengembangkan dan mengevaluasi model yang dirancang untuk memperkuat pertahanan jaringan medis dari ancaman siber [6].

2.1.13 *Confussion Matrix*

Metode *Confusion Ma*[illegible]akan untuk menghitung akurasi algoritma klasifikasi. Metode ini menghasilkan nilai-nilai seperti akurasi, presisi, dan *recall.* Akurasi adalah persentase ketepatan klasifikasi data yang berhasil dikelompokkan dengan benar setelah pengujian dilakukan [20]. Penelitian ini mengukur tingkat akurasi menggunakan metode *confusion matrix* yang ditunjukkan pada table 2.1 dibawah ini.

Tabel 2. 1 *Confussion Matrix*

Kategori		**Nilai Sebenarnya**	
		Benar	Salah
Nilai Prediksi	Benar	TP	FP
	Salah	FN	TN

Sumber: Jalil et al. 2024

Keterangan :

TP : Klasifikasi benar pada prediksi dan benar pada nilai sebenarnya

FP : Klasifikasi benar pada prediksi dan salah pada nilai sebenarnya

FN : Klasifikasi salah pada prediksi dan benar pada nilai sebenarnya

TN : Klasifikasi salah pada prediksi dan salah pada nilai sebenarnya

2.2 Penelitian Terdahulu yang Relevan

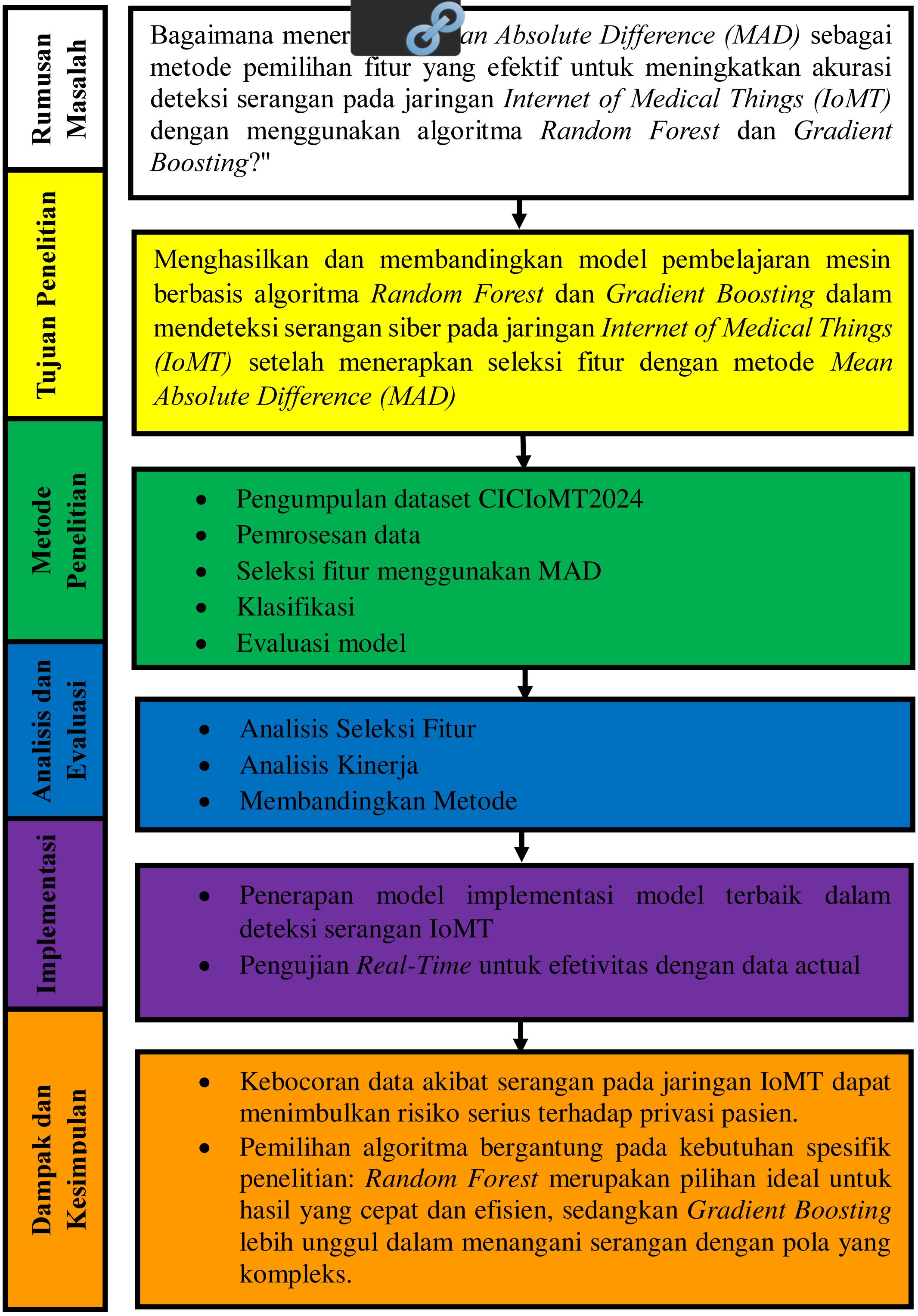
Berikut merupakan b[illegible]enelitian terdahulu yang menjadi landasan penelitian.

Tabel 2. 2 Penelitian Relevan

No.	Penulis	Judul	Metode	Hasil
1	Aljumaie, G. S., et al. (2021) [1]	*Modern Study on Internet of Medical Things (IoMT) Security*	*Analisis Literatur*	Identifikasi ancaman utama pada IoMT, termasuk risiko keamanan data, serta rekomendasi teknologi keamanan berbasis *blockchain* dan *enkripsi.*
2	Ghubaish, A., et al. (2020) [3]	*Recent Advances in the Internet-of-Medical-Things (IoMT) Systems Security*	*Kombinasi Blockchain dan Keamanan IoMT*	*Blockchain* terbukti efektif dalam mitigasi serangan siber pada perangkat IoMT, meskipun tantangan *interoperabilitas* masih menjadi kendala.
3	Adnan, A., et al. (2021) [7]	*An Intrusion Detection System for the Internet of Things Based on Machine Learning: Review and Challenges*	*Machine Learning*	Mengulas IDS berbasis machine learning untuk mendeteksi serangan pada IoT, dengan fokus pada tantangan dataset besar dan evaluasi akurasi.
4	Sun, Y., et al. (2019) [5]	*Security and Privacy for the Internet of Medical Things Enabled Healthcare Systems: A Survey*	*Survei literatur*	Menganalisis ancaman privasi dan keamanan pada IoMT, serta memberikan rekomendasi solusi berbasis kriptografi dan autentikasi.
5	Upadhyay et al. (2020) [12]	*Gradient boosting feature selection with machine learning classifiers for intrusion detection on power grids*	*Gradient Boosting, Feature Selection*	*Gradient Boosting* efektif untuk seleksi fitur dan klasifikasi serangan pada jaringan listrik, dengan tingkat akurasi tinggi.

2.3 Kerangka Berpikir

Berikut dibawah ini a[illegible] kerangka berpikir yang menjadi acuan dalam metodologi penelitian ini.



Bagaimana mener[illegible]an Absolute Difference (MAD)* sebagai metode pemilihan fitur yang efektif untuk meningkatkan akurasi deteksi serangan pada jaringan *Internet of Medical Things (IoMT)* dengan menggunakan algoritma *Random Forest* dan *Gradient Boosting*?"

Menghasilkan dan membandingkan model pembelajaran mesin berbasis algoritma *Random Forest* dan *Gradient Boosting* dalam mendeteksi serangan siber pada jaringan *Internet of Medical Things (IoMT)* setelah menerapkan seleksi fitur dengan metode *Mean Absolute Difference (MAD)*

- Pengumpulan dataset CICIoMT2024
- Pemrosesan data
- Seleksi fitur menggunakan MAD
- Klasifikasi
- Evaluasi model

- Analisis Seleksi Fitur
- Analisis Kinerja
- Membandingkan Metode

- Penerapan model implementasi model terbaik dalam deteksi serangan IoMT
- Pengujian *Real-Time* untuk efetivitas dengan data actual

- Kebocoran data akibat serangan pada jaringan IoMT dapat menimbulkan risiko serius terhadap privasi pasien.
- Pemilihan algoritma bergantung pada kebutuhan spesifik penelitian: *Random Forest* merupakan pilihan ideal untuk hasil yang cepat dan efisien, sedangkan *Gradient Boosting* lebih unggul dalam menangani serangan dengan pola yang kompleks.

Gambar 2. 6 Kerangka Berpikir

BAB III

METODOLOGI PENELITIAN

3.1 Metode Penelitian

Metode penelitian yang digunakan penulis dalam penelitian ini adalah metode kuantitatif untuk menguji efektivitas metode *Mean Absolute Difference (MAD)* dalam seleksi fitur. Penelitian kuantitatif merupakan pendekatan ilmiah yang dilakukan secara sistematis untuk mempelajari bagian-bagian dan hubungan kausal dari suatu fenomena. Penelitian ini melibatkan pengumpulan data yang dapat diukur menggunakan teknik analisis berbasis statistik, matematika, atau metode komputasi. Pendekatan ini bertujuan untuk mengidentifikasi hubungan antar variabel, menjelaskan fenomena, atau menguji hipotesis secara objektif melalui analisis data numerik [21].

3.2 Metode Pengumpulan Data

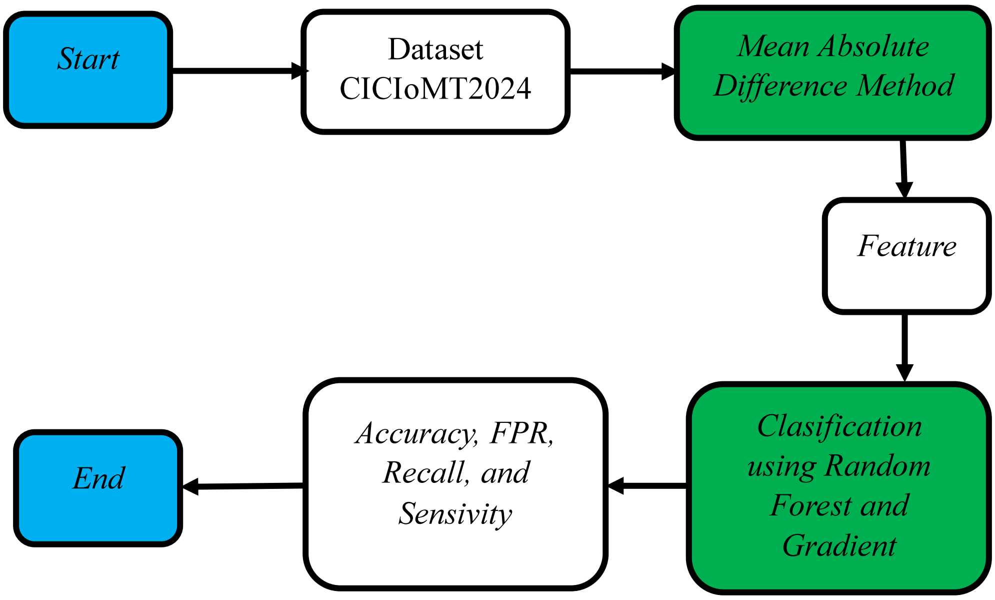
Dalam penelitian ini, pengumpulan data dilakukan melalui studi literatur untuk mengidentifikasi teori dan konsep yang relevan, serta pengolahan dataset yang akan digunakan. Metode pengumpulan data merujuk pada teknik atau prosedur yang diterapkan oleh peneliti untuk memperoleh data yang diperlukan guna mencapai tujuan penelitian. Pendekatan ini bertujuan untuk mengumpulkan informasi yang relevan dan mendukung proses analisis. Selain itu, instrumen yang digunakan dalam proses pengumpulan data dikenal sebagai alat atau sarana pengumpulan data.

Data yang digunakan dalam penelitian ini berupa dataset CICIoMT2024 dalam format CSV. Dataset ini dirancang khusus untuk mendukung penelitian terkait keamanan siber, dengan fokus pada jaringan *Internet of Medical Things (IoMT)*. CICIoMT2024 mencakup berbagai jenis data lalu lintas jaringan yang dihasilkan oleh perangkat IoMT, termasuk skenario aktivitas normal dan berbagai jenis serangan keamanan, sehingga cocok untuk tujuan analisis dan pengembangan model keamanan berbasis *Machine Learning*.

3.3 Metode Analisa

Metode analisis yang [illegible]akan dalam penelitian ini adalah analisis anomali. Pendekatan ini mer[illegible]lah satu metode utama dalam mendeteksi serangan pada jaringan ko[illegible] Metode analisis anomali berfokus pada identifikasi aktivitas atau perilaku yang tidak biasa dalam lalu lintas jaringan. Aktivitas yang mencurigakan ini dapat mencakup peningkatan mendadak dalam permintaan koneksi dari sumber yang tidak dikenal atau lonjakan volume lalu lintas dari alamat yang tidak dikenali.

Pendekatan yang digunakan dalam penelitian ini yaitu pendekatan *Machine Learning*, dengan menggunakan algoritma *Random Forest* dan *Gradient Boosting*, untuk klasifikasi serangan pada dataset CICIoMT2024 [6]. Penelitian ini akan dimulai dengan menjelaskan dataset yang digunakan, termasuk sumber, struktur, dan karakteristiknya. Selanjutnya, penelitian ini akan menerapkan metode *Machine Learning* dengan pendekatan seleksi fitur menggunakan *Mean Absolute Difference (MAD).* Metode ini bertujuan untuk memilih fitur yang relevan dalam deteksi serangan, sebelum menggunakan algoritma *Random Forest* dan *Gradient Boosting* untuk proses klasifikasi.



Gambar 3. 1 Tahapan proses penelitian

Dalam penelitian ini, tahapan-tahapan dari analisis kebutuhan antara lain:

a. Mulai *(Start)*

b. Dataset CICIoM[illegible]

Pada tahap ini, penulis mengumpulkan data yang diperlukan yaitu dataset *CICIoMT2024*, yang bertujuan untuk mendapatkan informasi tentang kebutuhan dari penulis dan analisis yang dibutuhkan.

c. *Mean Absolute Difference method*

Langkah selanjutnya adalah memilih fitur yang relevan, dalam analisis ini fitur yang dipilih menggunakan metode *Mean Absolute Difference.*

d. *Feature*

Setelah menggunakan fitur *Mean Absolute Difference* Kemudian, fitur-fitur yang telah dipilih digunakan untuk melatih model *Machine Learning* dengan algoritma *Random Forest* dan *Gradient Boosting.*

e. *Classification Using Random Forest and Gradient Boosting*

Selanjutnya, pada tahap klasifikasi, digunakan dua algoritma, yaitu *Random Forest* dan *Gradient Boosting*, untuk membangun model prediktif yang mampu mengidentifikasi pola dalam data.

f. *Accuracy, FPR, Recall, and Sensitivity*

Tahap berikutnya untuk mengevaluasi performa model dalam mendeteksi serangan pada dataset CICIoMT2024 adalah dengan menghitung metrik seperti akurasi, *False Positive Rate (FPR), recall,* dan sensitivitas.

g. *End*

Pada tahap evaluasi, hasil pengukuran metrik dapat memberikan gambaran tentang performa model yang telah dibuat.

3.4 Tempat dan Waktu Penelitian

3.4.1 Tempat Penelitian

Tempat pene[illegible] dilakukan di Ruangan Kampus B, Lab Rekayasa Sistem Ko[illegible] [illegible]iversitas Bina Insan, di JL. Jendral Besar HM. Soeharto KM13 Kelurahan Lubuk Kupang Kecamatan Lubuklinggau Selatan I Kota Lubuklinggau Sumatera Selatan.

3.4.2 Waktu Penelitian

Dalam menyelesaikan proposal skripsi ini, waktu penelitian yang dibutuhkan oleh penulis dapat dilihat dari table 3.1 berikut ini:

Tabel 3. 1 Waktu penelitian

No	**Jenis Kegiatan**	**Waktu Kegiatan**											
		November 2024				**Desember 2024**				**Januari 2024**			
		1	**2**	**3**	**4**	**1**	**2**	**3**	**4**	**1**	**2**	**3**	**4**
1	Pengajuan Judul	■	■	■	■								
2	Analisa Kebutuhan				■	■							
3	Penulisan Proposal					■	■	■	■				
4	Bimbingan Proposal								■				
5	Ujian Proposal								■				
6	Revisi ujian proposal								■				
7	Pengolahan dan pengujian data									■	■		
8	Bimbingan skripsi										■	■	
9	Ujian skripsi												■

3.5 Alat dan Bahan

3.5.1 Alat

Adapun alat yang di [illegible] enulis dalam penelitian ini adalah sebagai Berikut:

a. Perangkat Keras *(Hardware)*
   1. Laptop Acer
   2. Printer Epson L3210

b. Perangkat Lunak *(Software)*
   1. Microsoft Office Word 2019
   2. Python

3.5.2 Bahan

Adapun bahan yang digunakan penulis dalam penelitian ini adalah sebagai berikut:

a. Kertas A4 ukuran 70gram.

b. Tinta Printer.

3.6 Metode Pengujian dan pengolahan Data

3.6.1 Metode Pengujian

Metode pengujian dalam penelitian ini menggunakan *algoritma Random Forest* dan *Gradient Boosting* serta pemilihan fitur *Mean Absolute Difference (MAD)* untuk menilai kinerja sistem dalam mendeteksi serangan pada *Internet of Medical Things (IoMT).* Untuk memastikan bahwa data mencakup berbagai jenis serangan dan data normal yang *representatif*, pengujian pertama dilakukan pada dataset. Pengujian dilakukan berdasarkan kualitas, distribusi kelas, dan kelengkapan fitur setelah tahap *preprocessing* dan pemilihan fitur, di mana *Mean Absolute Difference (MAD)* digunakan.

Tahap berikutnya adalah melakukan pengujian pada proses *preprocessing* untuk memastikan bahwa data telah melalui tahap pembersihan, normalisasi, dan encoding dengan benar. Pengujian ini meliputi pengecekan keberadaan nilai yang hilang *(missing values)*, *verifikasi* skala data sete[illegible]malisasi, serta *validasi* hasil *encoding* pada fitur kategorikal. Selar[illegible]emilihan fitur dilakukan menggunakan metode *Mean Absolute* [illegible]*ce* dengan menghitung nilai statistiknya untuk memastikan bahwa fitur-fitur yang dipilih mampu meningkatkan performa model klasifikasi.

Evaluasi model klasifikasi dilakukan dengan melatih algoritma *Random Forest* dan *Gradient Boosting*. Untuk memastikan hasil yang konsisten, model ini diuji melalui *cross-validation* dan kemudian diuji pada data uji yang berbeda. Performa model diukur dengan metrik seperti:

1. *Akurasi*

   Dalam akurasi, menunjukkan seberapa akurat prediksi model dapat diklasifikasikan secara akurat dengan menggunakan kumpulan data [22].

   $$\frac{TP+TN}{TP+TN+FP+FN} \text{..} (1)$$

2. *Precision*

   Mengevaluasi tingkat keakuratan hasil data tertentu dengan membandingkan hasil yang dihasilkan oleh model yang menghitung perbedaan antara jumlah data dengan label positif dan jumlah data true positif [22].

   $$\frac{TP}{TP+FP} \text{...} (2)$$

3. *F1 Score*

   Perbandingan nilai rata-rata harmonik yang diperoleh dari hasil recall dan precision [22].

   $$F1 = 2\left(\frac{Precession * Recall}{Precession + Recall}\right) \text{........................} (3)$$

4. *False Positive Rate (FPR)*

   FPR adalah ukuran [illegible]a sering model memprediksi kelas negatif untuk data yang se[illegible] FPR dapat dihitung dengan membagi jumlah prediksi kel[illegible] yang salah dengan jumlah total kelas negatif [22].

   $$\frac{FP}{FP+TN} \text{..} \tag{4}$$

5. *True Positive Rate (TPR)*

   (TPR) yang juga dikenal sebagai sensitivitas atau *recall*, adalah metrik yang mengukur seberapa baik model mendeteksi label positif yang sebenarnya. TPR dihitung dengan membagi jumlah prediksi benar untuk kelas positif *(True Positive)* dengan total jumlah data yang benar-benar termasuk dalam kelas positif *(True Positive + False Negative)* [22].

   $$\frac{TP}{TP+FN} \text{..} \tag{5}$$

6. *True Negative Rate (TNR)*

   TNR juga dikenal sebagai *specificity*, adalah metrik yang digunakan untuk mengukur kemampuan suatu model dalam mengidentifikasi data negatif dengan benar. TNR menunjukkan proporsi dari data yang sebenarnya negatif *(True Negative)* yang berhasil diprediksi dengan tepat oleh model terhadap total jumlah data negatif [22].

   $$\frac{TN}{TP+FN} \text{..} \tag{6}$$

7. *False Negative Rate (FNR)*

   FNR adalah metrik yang digunakan untuk mengukur seberapa sering model salah memprediksi data yang sebenarnya termasuk dalam kelas negatif sebagai kelas positif [22].

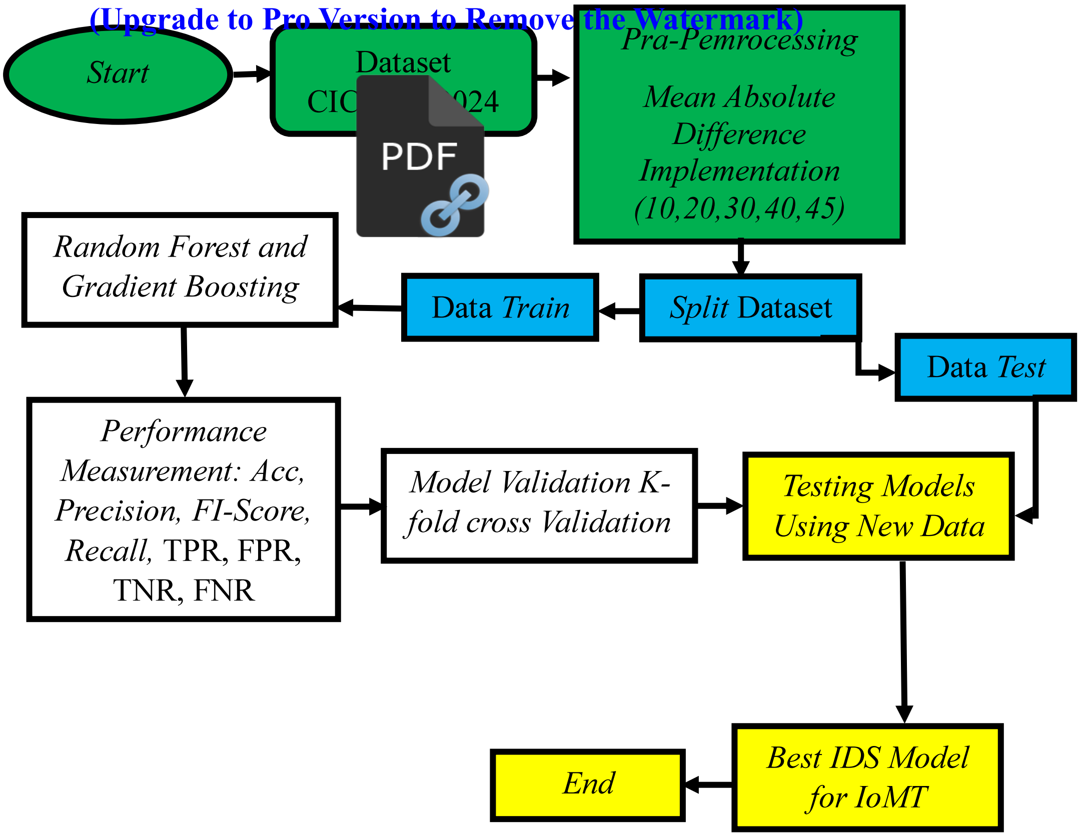
   $$\frac{FN}{TP+FN} \text{..} \tag{7}$$

Hasil evaluasi dari kedua algoritma dibandingkan untuk menentukan mana yang lebih unggul antar[illegible]m *Forest* dan *Gradient Boosting*.

Hasil pengujian [illegible] dalam bentuk visualisasi yang mencakup tabel, grafik, dan *co[illegible]atrix* untuk mendukung analisis dan interpretasi data. Visualisasi ini memberikan gambaran yang jelas mengenai performa sistem dalam mendeteksi serangan pada jaringan IoMT. Berdasarkan hasil pengujian, dilakukan evaluasi untuk menentukan tingkat keberhasilan sistem dalam mencapai akurasi tinggi.

3.6.2 Pengolahan Data

Sebelum data dibagi menjadi data latih dan data uji, data yang dikumpulkan terlebih dahulu diproses melalui tahap pembersihan, *encoding,* dan normalisasi. *Metode Mean Absolute Difference* digunakan untuk memilih fitur-fitur yang signifikan dalam pelatihan model. *Gradient Boosting* bekerja dengan iterasi untuk memperbaiki kesalahan pada model sebelumnya, sedangkan *Random Forest* menggabungkan hasil dari berbagai pohon keputusan. Evaluasi kinerja kedua model dilakukan menggunakan metrik seperti akurasi, presisi, dan *recall*. Hasil analisis menunjukkan bahwa pemilihan fitur yang tepat secara signifikan dapat meningkatkan kinerja model dalam mendeteksi serangan dengan membandingkan keunggulan masing-masing algoritma. Hasilnya menunjukkan bahwa, dengan membandingkan keunggulan masing-masing algoritma, pemilihan fitur yang tepat dapat meningkatkan kinerja deteksi serangan. Pada Gambar 3.2 merupakan tahapan-tahapan dalam pengolahan data *training* dan data *testing*.

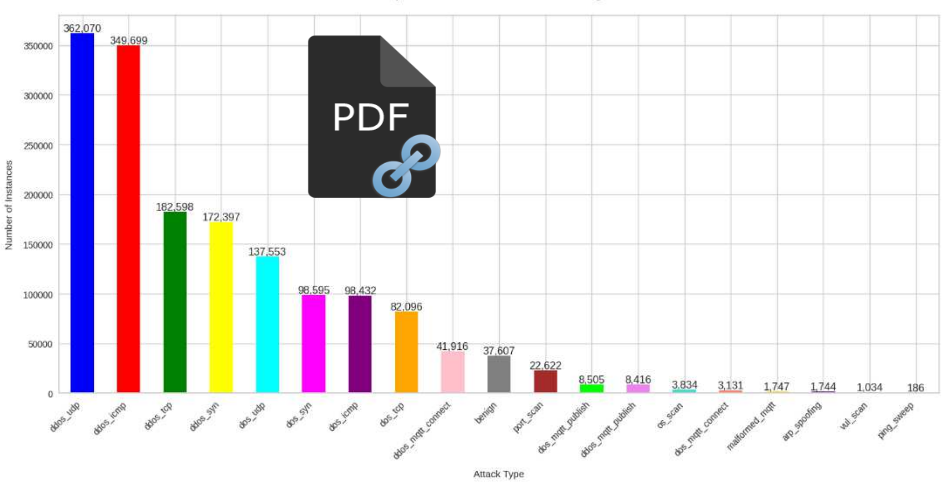


Gambar 3. 2 *Flowchart* Menentukan model terbaik

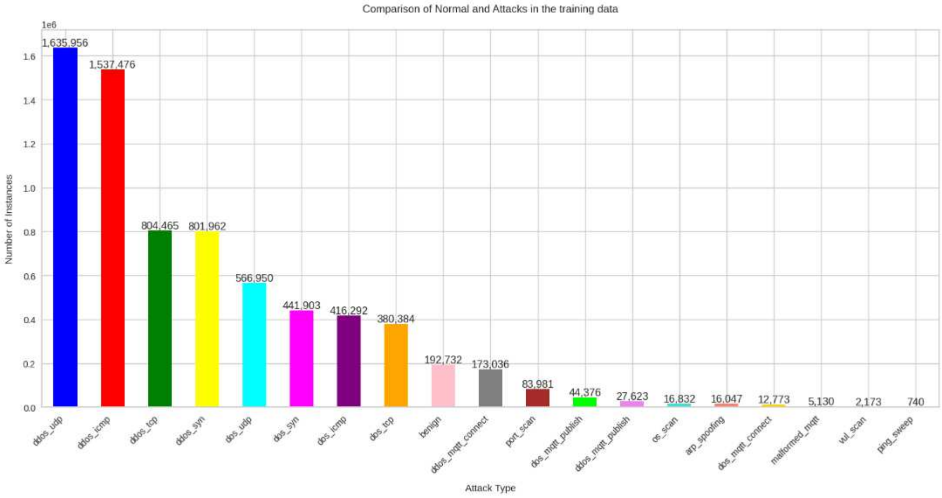
Dalam penelitian ini, tahapan-tahapan dari Pengolahan data antara lain:

1. *Start*
2. Dataset CICIoMT2024

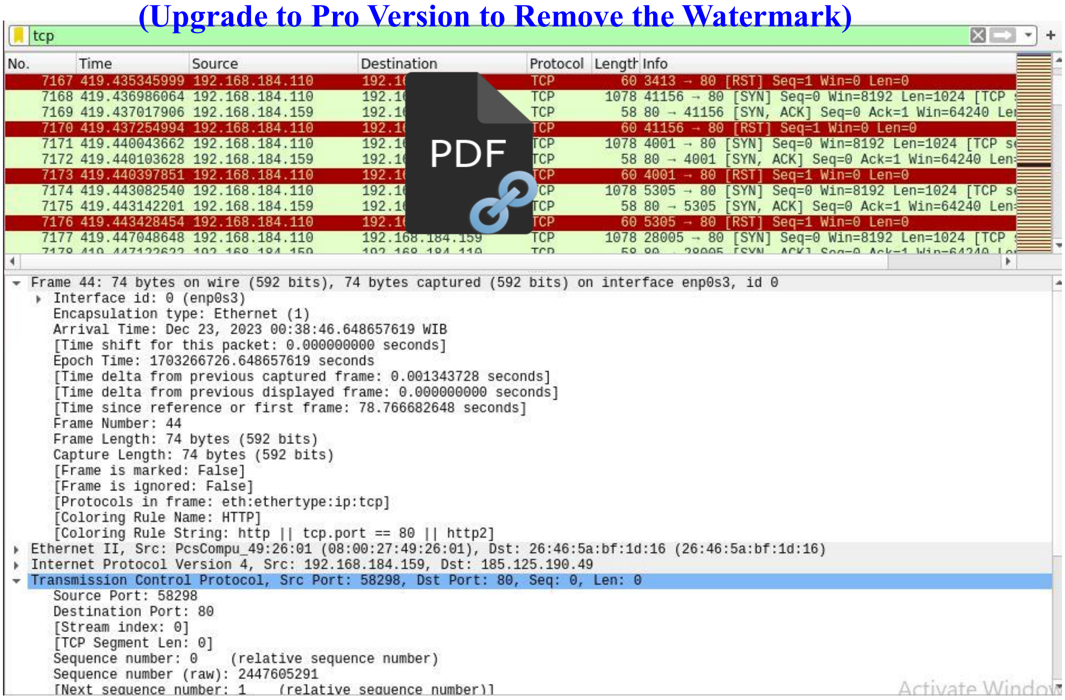
   Pada tahap ini, penulis mengumpulkan data yang diperlukan yaitu dataset *CICIoMT2024*, yang bertujuan untuk mendapatkan informasi tentang kebutuhan dari penulis dan analisis yang dibutuhkan, lalu menentukan *class attack* dari *testing* dan *training* data dalam dataset seperti Gambar 3.3 dan Gambar 3.4 dibawah ini:



***Gambar 3. 3** Class attack testing data*



Gambar 3. 4 *Class attack training data*



```
7167 419.435345999 192.168.184.110   192.16   TCP     60 3413 → 80 [RST] Seq=1 Win=0 Len=0
7168 419.436986064 192.168.184.110   192.16   TCP   1078 41156 → 80 [SYN] Seq=0 Win=8192 Len=1024 [TCP
7169 419.437017906 192.168.184.159   192.16   TCP     58 80 → 41156 [SYN, ACK] Seq=0 Ack=1 Win=64240 Le
7170 419.437254994 192.168.184.110   192.16   TCP     60 41156 → 80 [RST] Seq=1 Win=0 Len=0
7171 419.440043662 192.168.184.110   192.16   TCP   1078 4001 → 80 [SYN] Seq=0 Win=8192 Len=1024 [TCP se
7172 419.440103628 192.168.184.159   192.16   TCP     58 80 → 4001 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len
7173 419.440397851 192.168.184.110   192.16   TCP     60 4001 → 80 [RST] Seq=1 Win=0 Len=0
7174 419.443082540 192.168.184.110   192.16   TCP   1078 5305 → 80 [SYN] Seq=0 Win=8192 Len=1024 [TCP se
7175 419.443142201 192.168.184.159   192.16   TCP     58 80 → 5305 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len
7176 419.443428454 192.168.184.110   192.16   TCP     60 5305 → 80 [RST] Seq=1 Win=0 Len=0
7177 419.447048648 192.168.184.110   192.168.184.159   TCP   1078 28005 → 80 [SYN] Seq=0 Win=8192 Len=1024 [TCP
```

```
Frame 44: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface enp0s3, id 0
  Interface id: 0 (enp0s3)
  Encapsulation type: Ethernet (1)
  Arrival Time: Dec 23, 2023 00:38:46.648657619 WIB
  [Time shift for this packet: 0.000000000 seconds]
  Epoch Time: 1703266726.648657619 seconds
  [Time delta from previous captured frame: 0.001343728 seconds]
  [Time delta from previous displayed frame: 0.000000000 seconds]
  [Time since reference or first frame: 78.766682648 seconds]
  Frame Number: 44
  Frame Length: 74 bytes (592 bits)
  Capture Length: 74 bytes (592 bits)
  [Frame is marked: False]
  [Frame is ignored: False]
  [Protocols in frame: eth:ethertype:ip:tcp]
  [Coloring Rule Name: HTTP]
  [Coloring Rule String: http || tcp.port == 80 || http2]
Ethernet II, Src: PcsCompu_49:26:01 (08:00:27:49:26:01), Dst: 26:46:5a:bf:1d:16 (26:46:5a:bf:1d:16)
Internet Protocol Version 4, Src: 192.168.184.159, Dst: 185.125.190.49
Transmission Control Protocol, Src Port: 58298, Dst Port: 80, Seq: 0, Len: 0
  Source Port: 58298
  Destination Port: 80
  [Stream index: 0]
  [TCP Segment Len: 0]
  Sequence number: 0    (relative sequence number)
  Sequence number (raw): 2447605291
  [Next sequence number: 1    (relative sequence number)]
```

Gambar 3. 5 Contoh serangan pada *Class attack type dos syn*

3. *Pra-Pemrocessing*

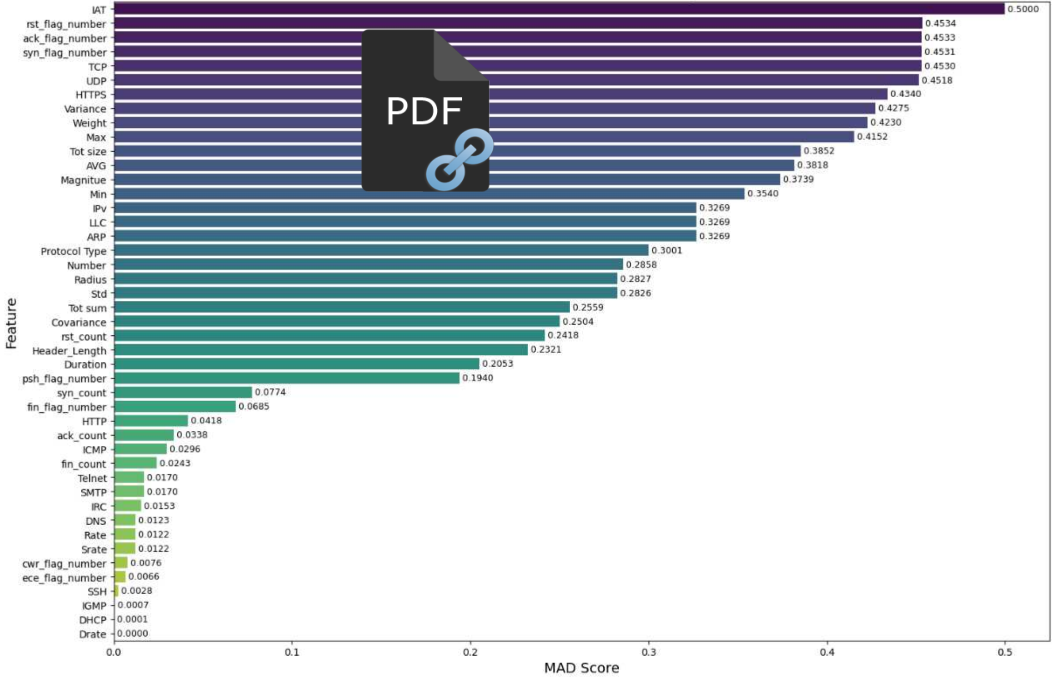
   Setelah dataset dikumpulkan selanjutnya adalah pra-pemrosesan dengan menentukan nilai dari setiap fitur berdasarkan *Mean Absolute Difference* yang merupakan metode yang digunakan dalam analisis dataset CICIoMT2024.Fitur fitur tersebut diseleksi dari 10 fitur sampai 45 fitur, seperti pada tabel 3.2 dan tabel 3.3, gambar grafik 3.6 dan gambar grafik 3.7:

Tabel 3. 2 Bobot nilai fitur pada data train

Rank	***[illegible]re***	***Mean Absolute Difference Score***
1	IAT *(Inter-Arrival Time)*	0.499988
2	rst_flag_number *(Reset Flag Count)*	0.453422
3	ack_flag_number *(Acknowledgment Flag Count)*	0.453344
4	syn_flag_number *(Synchronization Flag Count)*	0.453100
5	TCP *(Transmission Control Protocol)*	0.453013
6	UDP *(User Datagram Protocol)*	0.451794
7	HTTPS *(HyperText Transfer Protocol Secure)*	0.433977
8	Variance	0.427457
9	Weight	0.423042
10	Max *(Maximum)*	0.415186
11	Tot size *(Total Size)*	0.385237
12	AVG *(Average)*	0.381761
13	Magnitue	0.373869
14	Min *(Minimum)*	0.354019

15	Ipv *(Internet Protocol [illegible]n)*	0.326888
16	LLC *(L[illegible]k Control)*	0.326888
17	ARP *(Address Resolution Protocol)*	0.326888
18	Protocol Type	0.300070
19	Number	0.285763
20	Radius	0.282676
21	Std *(Standard Deviation)*	0.282587
22	Tot sum *(Total Sum)*	0.255855
23	Covariance	0.250390
24	rst_count *(Reset Packet Count)*	0.241799
25	Header_Length	0.232087
26	Duration	0.205287
27	psh_flag_number *(Push Flag Count)*	0.193998
28	syn_count *(Synchronization Packet Count)*	0.077385
29	fin_flag_number *(Finish Flag Count)*	0.068509
30	HTTP *(HyperText Transfer Protocol)*	0.041826
31	ack_count *(Acknowledgment Packet Count)*	0.033779

32	ICMP *(Internet Control Me[illegible]rotocol)*	0.029592
33	fin_co[illegible]*h Packet*	0.024306
34	Telnet *(Terminal Network)*	0.016964
35	SMTP *(Simple Mail Transfer Protocol)*	0.016964
36	IRC *(Internet Relay Chat)*	0.015267
37	DNS *(Domain Name System)*	0.012266
38	Rate	0.012214
39	Srate *(Source Rate)*	0.012214
40	cwr_flag_number *(Congestion Window Reduced Flag Count)*	0.007576
41	ece_flag_number *(Explicit Congestion Notification Echo Flag Count)*	0.006551
42	SSH *(Secure Shell)*	0.002771
43	IGMP (Internet Group Management Protocol)	0.000657
44	DHCP *(Dynamic Host Configuration Protocol)*	0.000145
45	Drate *(Destination Rate)*	0.000000



Gambar 3. 6 Grafik *Train* Data

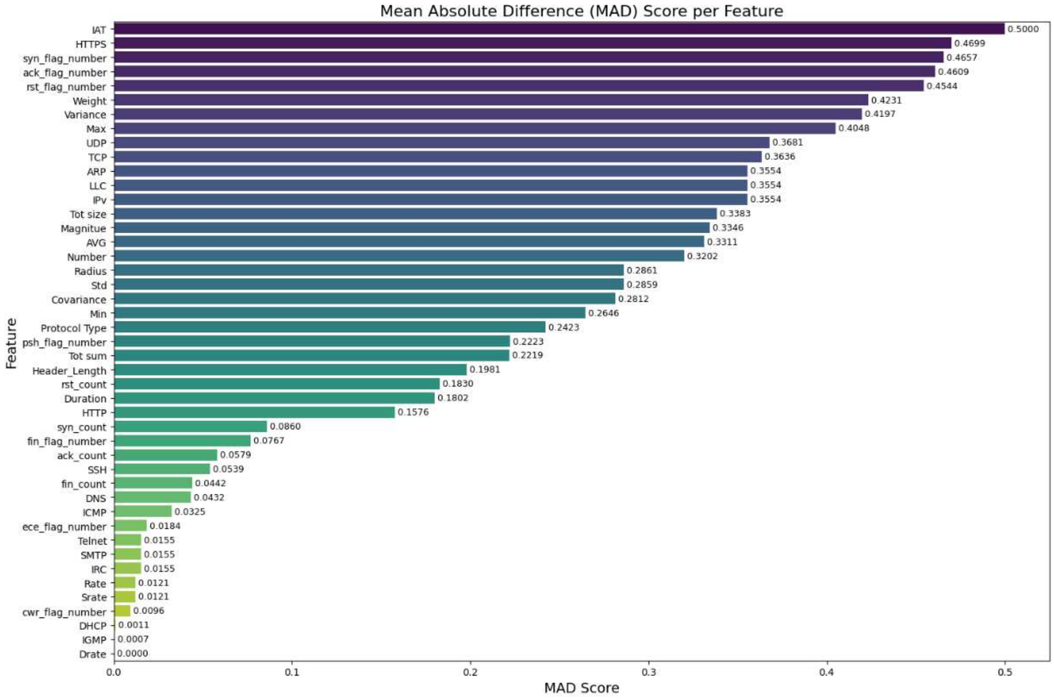
Tabel 3. 3 Bobot nilai fitur pada data *test*

Rank	***Feature***	***Mean Absolute Difference Score***
1	IAT *(Inter-Arrival Time)*	0.499988
2	HTTPS *(HyperText Transfer Protocol Secure)*	0.469943
3	syn_flag_number *(Synchronization Flag Count)*	0.465698
4	ack_flag_number *(Acknowledgment Flag Count)*	0.460906
5	rst_flag_number *(Reset Flag Count)*	0.454429

6	Weight	0.423114
7	[illegible]e	0.419719
8	M[illegible]*num)*	0.404810
9	UDP *(User Datagram Protocol)*	0.368058
10	TCP *(Transmission Control Protocol)*	0.363649
11	ARP *(Address Resolution Protocol)*	0.355394
12	LLC *(Logical Link Control)*	0.355394
13	Ipv *(Internet Protocol Version)*	0.355394
14	Tot size *(Total Size)*	0.338310
15	Magnitue	0.334563
16	AVG *(Average)*	0.331141
17	Number	0.320183
18	Radius	0.286110
19	Std *(Standard Deviation)*	0.285950
20	Covariance	0.281181
21	Min *(Minimum)*	0.264579
22	Protocol Type	0.242288
23	psh_flag_number *(Push Flag Count)*	0.222287

24	Tot sum *(Total Sum)*	0.221880
25	H[illegible]ngth	0.198064
26	rst_count [illegible]*cket Count)*	0.182966
27	Duration	0.180176
28	HTTP *(HyperText Transfer Protocol)*	0.157550
29	syn_count *(Synchronization Packet Count)*	0.085958
30	fin_flag_number *(Finish Flag Count)*	0.076665
31	ack_count *(Acknowledgment Packet Count)*	0.057852
32	SSH *(Secure Shell)*	0.053919
33	fin_count *(Finish Packet Count)*	0.044200
34	DNS *(Domain Name System)*	0.043220
35	ICMP *(Internet Control Message Protocol)*	0.032466
36	ece_flag_number *(Explicit Congestion Notification Echo Flag Count)*	0.018432
37	Telnet *(Terminal Network)*	0.015527
38	SMTP *(Simple Mail Transfer Protocol)*	0.015527
39	IRC *(Internet Relay Chat)*	0.015527

40	Rate	0.012144
41	Srat [illegible] *Rate)*	0.012144
42	cwr_flag_ [illegible] *Congestion Window Reduced Flag Count)*	0.009560
43	DHCP *(Dynamic Host Configuration Protocol)*	0.001146
44	IGMP (Internet Group Management Protocol)	0.000664
45	Drate *(Destination Rate)*	0.000000



Gambar 3. 7 Grafik Test data

Berdasarkan skor *Mean Absolute Difference* pada tabel 3.2 dan tabel 3.3, gambar grafik 3.6 dan gambar grafik 3.7, menunjukkan bahwa semakin besar skor *Mean Absolute Difference* yang ada pada masing masing fitur maka semakin penting fitur tersebut.

4. *Split* dataset

   Selanjutnya untu[illegible]embangkan model *Machine Learning, split* dataset adalah p[illegible]mbagi dataset menjadi beberapa subset (data latih dan [illegible] untuk memastikan bahwa model dapat dilatih, dan diuji secara efisien. Data *test* berjumlah 1,614,182 data (18%), sedangkan data *train* berjumlah 7,160,831 data (82%). Jumlah data keseluruhan *train* dan *test* adalah 8,775,013 data.

5. Data *Train*

   Setelah dataset dibagi menjadi data latih *(train)* dan data uji *(test),* langkah berikutnya adalah memanfaatkan data latih terlebih dahulu untuk melatih model *machine learning*. Data latih ini merupakan bagian dari dataset yang digunakan untuk membantu algoritma dalam mengenali pola serta hubungan di dalam data sebelum model diuji menggunakan data uji.

6. *Random Forest and Gradient Boosting*

   Langkah berikutnya adalah memilih algoritma yang akan digunakan, antara *Random Forest* dan *Gradient Boosting,* untuk menentukan algoritma mana yang memberikan hasil lebih efisien dalam pemodelan.

7. *Performance measurement: Acc, Precision, F1-Score, Recall, TPR, FPR, TNR, FNR*

   Selanjutnya mengukur model dengan performa matrik seperti *acc, precision, F1-Score, Recall, TPR, FPR, TNR, FNR.*

8. Model *Validation K-Fold Cross Validation*

   Selanjutnya model diuji dengan *K-Fold Cross Validation* untuk menentukan hasil yang konsisten.

9. *Testing models using new data*

   Setelah dilakukan pengujian menggunakan model *K-Fold Cross Validation,* data uji *(testing)* dipisahkan untuk menghasilkan data baru. Data uji yang diperbarui ini kemudian digunakan untuk pengujian lebih lanjut.

10. Data *test*

    Setelah proses [illegible]han selesai, langkah berikutnya adalah menggunakan da[illegible]uk mengevaluasi kinerja model *machine learning*.

11. *Best IDS Model For IoMT*

    Setelah menyelesaikan semua tahapan di atas, kita akan memperoleh model IDS terbaik untuk *Internet of Medical Things (IoMT),* yang berperan penting dalam menjaga keamanan data pasien serta perangkat medis.

12. *End.*

BAB IV

HASIL PENELITIAN DAN PEMBAHASAN

4.1 Gambaran Umum

Penelitian ini berfokus pada deteksi serangan siber pada jaringan *Internet of Medical Things* (IoMT) menggunakan pendekatan *Mean Absolute Difference* (MAD) untuk seleksi fitur dan algoritma *Random Forest* serta *Gradient Boosting* untuk klasifikasi. Dataset yang digunakan adalah CICIoMT2024, yang dirancang untuk mendukung penelitian keamanan IoMT dengan mencakup 19 jenis serangan siber, seperti *Denial-of-Service* (DoS), *Distributed Denial-of-Service* (DDoS), dan *Man-in-the-Middle* (MitM).

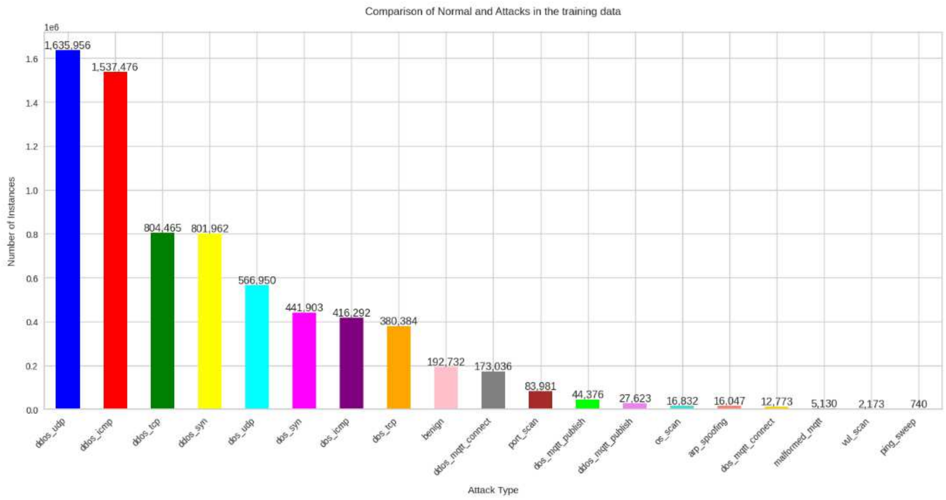
Pengolahan dataset dimulai dengan tahapan pra-pemrosesan, seperti pembersihan data, *encoding*, dan normalisasi. Seleksi fitur dilakukan menggunakan MAD untuk memilih fitur yang signifikan terhadap deteksi serangan. Model *machine learning* dilatih dengan algoritma *Random Forest* dan *Gradient Boosting*, diikuti evaluasi performa menggunakan metrik seperti akurasi, presisi, F1-*score*, *True Positive Rate* (TPR), *False Positive Rate* (FPR), dan lainnya. Hasil evaluasi ditampilkan dalam bentuk tabel, grafik, dan *confusion matrix* untuk memberikan gambaran performa model secara keseluruhan.

Dataset CICIoMT2024 yang digunakan dalam penelitian ini memainkan peran penting dalam mengidentifikasi pola serangan siber dan membangun model deteksi serangan yang akurat. Fokus utama penelitian ini adalah mengoptimalkan keamanan jaringan IoMT melalui pendekatan berbasis *machine learning* yang inovatif dan efektif.

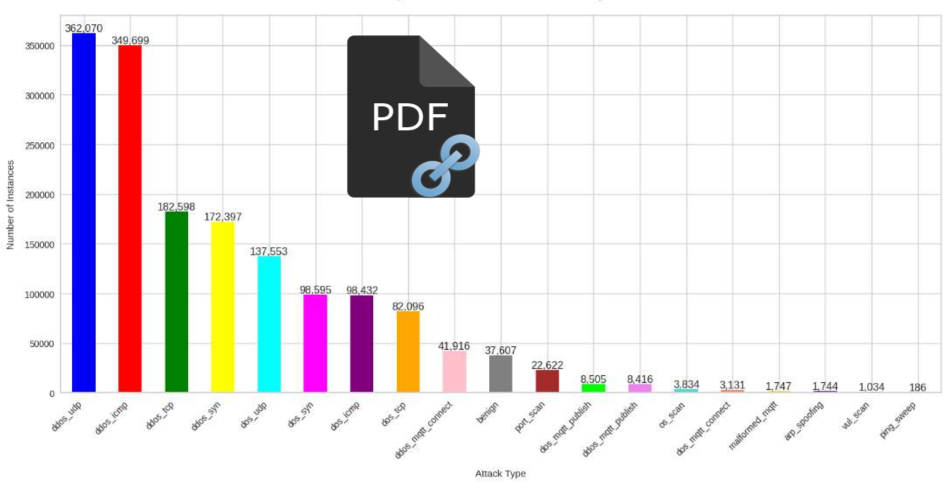
4.2 Hasil

4.2.1 Analisis Dataset

Pada penelitian ini, d CIoMT2024 digunakan untuk melatih dan menguji model *Random Fo* *Gradient Boosting*. Dataset ini terdiri dari 8.775.013 data, yang terbagi menjadi data latih (*train*) sebesar 82% dan data uji (*test*) sebesar 18%, dengan 45 fitur. Setelah seleksi fitur menggunakan *Mean Absolute Difference (MAD),* fitur dikurangi menjadi 10, 20, 30, dan 40 fitur terbaik berdasarkan skor MAD. Hasil evaluasi menunjukkan bahwa akurasi model tetap konsisten meskipun jumlah fitur dikurangi. Gambar 4.1 dan gambar 4.2 berikut menunjukkan distribusi kelas pada dataset *train* dan *test.*



Gambar 4. 1 Distribusi kelas data *train*



Gambar 4. 2 Distribusi kelas pada data *test*

4.2.2 Hasil Seleksi Fitur

Pada penelitian ini, penulis menerapkan *metode Mean Absolute Difference (MAD)* untuk menentukan fitur-fitur yang paling relevan dalam melatih model *machine learning*. Penelitian ini juga membandingkan kinerja model *machine learning* berdasarkan penggunaan 10, 20, 30, 40, dan tanpa pemilihan fitur dengan *score* tertinggi.

Tabel 4.1 dan Tabel 4.2 dibawah ini menunjukkan urutan fitur dengan *score* dari yang tertinggi hingga terendah yang akan digunakan sebagai fitur untuk melatih model *machine learning* dalam mendeteksi serangan di dalam dataset.

Tabel 4. 1 *Score* MAD untuk setiap fitur pada data latih

Rank	***Feature***	***Mean Absolute Difference Score***
1	IAT *(Inter-Arrival Time)*	0.499988
2	rst_flag_number *(Reset Flag Count)*	0.453422

3	ack_flag_number *(Acknowl*[illegible]*t Flag Count)*	0.453344
4	sy[illegible]mber *(Synchro*[illegible]*lag Count)*	0.453100
5	TCP *(Transmission Control Protocol)*	0.453013
6	UDP *(User Datagram Protocol)*	0.451794
7	HTTPS *(HyperText Transfer Protocol Secure)*	0.433977
8	Variance	0.427457
9	Weight	0.423042
10	Max *(Maximum)*	0.415186
11	Tot size *(Total Size)*	0.385237
12	AVG *(Average)*	0.381761
13	Magnitue	0.373869
14	Min *(Minimum)*	0.354019
15	Ipv *(Internet Protocol Version)*	0.326888
16	LLC *(Logical Link Control)*	0.326888
17	ARP *(Address Resolution Protocol)*	0.326888
18	Protocol Type	0.300070
19	Number	0.285763

20	Radius	0.282676
21	Std *(S* [illegible] *Deviation)*	0.282587
22	Tot [illegible] *l Sum)*	0.255855
23	Covariance	0.250390
24	rst_count *(Reset Packet Count)*	0.241799
25	Header_Length	0.232087
26	Duration	0.205287
27	psh_flag_number *(Push Flag Count)*	0.193998
28	syn_count *(Synchronization Packet Count)*	0.077385
29	fin_flag_number *(Finish Flag Count)*	0.068509
30	HTTP *(HyperText Transfer Protocol)*	0.041826
31	ack_count *(Acknowledgment Packet Count)*	0.033779
32	ICMP *(Internet Control Message Protocol)*	0.029592
33	fin_count *(Finish Packet Count)*	0.024306
34	Telnet *(Terminal Network)*	0.016964
35	SMTP *(Simple Mail Transfer Protocol)*	0.016964
36	IRC *(Internet Relay Chat)*	0.015267

37	DNS *(Domain Name System)*	0.012266
38	[illegible]	0.012214
39	Srat[illegible] *Rate)*	0.012214
40	cwr_flag_number *(Congestion Window Reduced Flag Count)*	0.007576
41	ece_flag_number *(Explicit Congestion Notification Echo Flag Count)*	0.006551
42	SSH *(Secure Shell)*	0.002771
43	IGMP (Internet Group Management Protocol)	0.000657
44	DHCP *(Dynamic Host Configuration Protocol)*	0.000145
45	Drate *(Destination Rate)*	0.000000

Tabel 4. 2 *Score* MAD untuk setiap fitur pada data uji

Rank	***Feature***	***Mean Absolute Difference Score***
1	IAT *(Inter-Arrival Time)*	0.499988
2	HTTPS *(HyperText Transfer Protocol Secure)*	0.469943
3	syn_flag_number *(Synchronization Flag Count)*	0.465698
4	ack_flag_number *(Acknowledgment Flag Count)*	0.460906

5	rst_flag_number *(Reset Flag* [illegible]*t)*	0.454429
6	[illegible]	0.423114
7	Variance	0.419719
8	Max *(Maximum)*	0.404810
9	UDP *(User Datagram Protocol)*	0.368058
10	TCP *(Transmission Control Protocol)*	0.363649
11	ARP *(Address Resolution Protocol)*	0.355394
12	LLC *(Logical Link Control)*	0.355394
13	Ipv *(Internet Protocol Version)*	0.355394
14	Tot size *(Total Size)*	0.338310
15	Magnitue	0.334563
16	AVG *(Average)*	0.331141
17	Number	0.320183
18	Radius	0.286110
19	Std *(Standard Deviation)*	0.285950
20	Covariance	0.281181
21	Min *(Minimum)*	0.264579
22	Protocol Type	0.242288

23	psh_flag_number *(Push Flag* [illegible]*t)*	0.222287
24	Tot [illegible] *l Sum)*	0.221880
25	Header_Length	0.198064
26	rst_count *(Reset Packet Count)*	0.182966
27	Duration	0.180176
28	HTTP *(HyperText Transfer Protocol)*	0.157550
29	syn_count *(Synchronization Packet Count)*	0.085958
30	fin_flag_number *(Finish Flag Count)*	0.076665
31	ack_count *(Acknowledgment Packet Count)*	0.057852
32	SSH *(Secure Shell)*	0.053919
33	fin_count *(Finish Packet Count)*	0.044200
34	DNS *(Domain Name System)*	0.043220
35	ICMP *(Internet Control Message Protocol)*	0.032466
36	ece_flag_number *(Explicit Congestion Notification Echo Flag Count)*	0.018432
37	Telnet *(Terminal Network)*	0.015527
38	SMTP *(Simple Mail Transfer Protocol)*	0.015527

39	IRC *(Internet Relay Chat)*	0.015527
40	[illegible]	0.012144
41	Srat[illegible] *Rate)*	0.012144
42	cwr_flag_number *(Congestion Window Reduced Flag Count)*	0.009560
43	DHCP *(Dynamic Host Configuration Protocol)*	0.001146
44	IGMP (Internet Group Management Protocol)	0.000664
45	Drate *(Destination Rate)*	0.000000

4.3 Pembahasan

4.3.1 Pengukuran Performa Klasifikasi

Evaluasi kinerja model *Intrusion Detection System (IDS)* dilakukan untuk menilai kemampuan model dalam mendeteksi ancaman siber pada jaringan IoMT. Berdasarkan hasil penelitian, setiap model IDS yang dibangun menggunakan algoritma yang berbeda menunjukkan tingkat akurasi terbaiknya. Tabel 4.3 dan Tabel 4.4 menyajikan perbandingan akurasi model IDS untuk algoritma *random forest* dan *gradient boosting* pada data latih dan data uji. Hasil perbandingan ini mengilustrasikan efektivitas berbagai teknik pembelajaran mesin dalam mengidentifikasi potensi ancaman pada jaringan IoMT.

Tabel 4. 3 Akurasi model ML 10 sampai Tanpa pemilihan fitur data latih

Classifier	***Accuracy***
Random Forest 10* fitur *train	100 %
Random Forest 20* fitur *train	100 %
Random Forest 30* fitur *train	100 %
Random Forest 40* fitur *train	100 %
RF* tanpa pemilihan fitur *train	100 %
GB* tanpa pemilihan fitur *train	99,3 %

Tabel 4. 4 Akurasi model ML 10 sampai Tanpa pemilihan fitur data uji

Classifier	*Accuracy*
***Random Forest 10* fitur**	100 %
***Random Forest 20* fitur**	100 %
***Random Forest 30* fitur**	100 %
Random Forest 40* fitur *test	100 %
RF tanpa pemilihan fitur *test*	100 %
GB tanpa pemilihan fitur *test*	99,3 %

Hasil klasifikasi menunjukkan bahwa algoritma *Random Forest* mencapai akurasi hingga 100 %, sedikit lebih tinggi dibandingkan *Gradient Boosting*, yang memiliki akurasi 99,3 %. *Random Forest* menunjukkan keunggulan yang luar biasa dalam memprediksi data, berkat kemampuannya untuk menangani sejumlah besar fitur secara efektif dan ketahanannya terhadap masalah *overfitting*. Sementara itu, *Gradient Boosting* juga menunjukkan performa yang sangat baik meskipun sedikit lebih rendah, dengan kemampuan mengatasi *overfitting* melalui pendekatan bertahap dalam pembelajaran. Mengingat kedua model memiliki tingkat akurasi yang tinggi, *Random Forest* menjadi pilihan yang lebih unggul untuk solusi ini karena menghasilkan prediksi yang sedikit lebih akurat.

Tabel 4.5 sampai Tabel 4.9 menunjukkan kinerja model *machine learning* menggunakan algoritma *Random Forest* pada data latih.

Tabel 4. 5 *Random Forest* 10 fitur data latih

Class	**Precision**	**F1-Score**	**TPR**	**FPR**	**TNR**	**FNR**
arp_spoofing	0.99	0.99	0.9802	0.0000	1.0000	0.0198
benign	1.00	1.00	0.9992	0.0001	0.9999	0.0008
ddos_icmp	1.00	1.00	1.0000	0.0000	1.0000	0.0000
ddos_mqtt_connect	1.00	1.00	1.0000	0.0000	1.0000	0.0000
ddos_mqtt_publish	1.00	1.00	1.0000	0.0000	1.0000	0.0000
ddos_syn	1.00	1.00	1.0000	0.0000	1.0000	0.0000

ddos_tcp	1.00	1.00	1.0000	0.0000	1.0000	0.0000
ddos_udp	1.00	1.00	1.0000	0.0000	1.0000	0.0000
dos_icmp	1.00	1.00	1.0000	0.0000	1.0000	0.0000
dos_mqtt_connect	1.00	1.00	1.0000	0.0000	1.0000	0.0000
dos_mqtt_publish	1.00	1.00	1.0000	0.0000	1.0000	0.0000
dos_syn	1.00	1.00	1.0000	0.0000	1.0000	0.0000
dos_tcp	1.00	1.00	1.0000	0.0000	1.0000	0.0000
dos_udp	1.00	1.00	1.0000	0.0000	1.0000	0.0000
malformed_mqtt	0.98	0.98	0.9680	0.0000	1.0000	0.0320
os_scan	0.98	0.87	0.7876	0.0000	1.0000	0.2124
ping_sweep	1.00	0.99	0.9824	0.0000	1.0000	0.0176
port_scan	0.96	0.98	0.9954	0.0005	0.9995	0.0046
vul_scan	0.99	0.94	0.8951	0.0000	1.0000	0.1049

Tabel 4. 6 *Random Forest* 20 fitur data latih

Class	**Precision**	**F1-Score**	**TPR**	**FPR**	**TNR**	**FNR**
arp_spoofing	0.99	0.99	0.9874	0.0000	1.0000	0.0126
benign	1.00	1.00	0.9993	0.0001	0.9999	0.0007
ddos_icmp	1.00	1.00	1.0000	0.0000	1.0000	0.0000
ddos_mqtt_connect	1.00	1.00	1.0000	0.0000	1.0000	0.0000
ddos_mqtt_publish	1.00	1.00	1.0000	0.0000	1.0000	0.0000
ddos_syn	1.00	1.00	1.0000	0.0000	1.0000	0.0000
ddos_tcp	1.00	1.00	1.0000	0.0000	1.0000	0.0000
ddos_udp	1.00	1.00	1.0000	0.0000	1.0000	0.0000
dos_icmp	1.00	1.00	1.0000	0.0000	1.0000	0.0000
dos_mqtt_connect	1.00	1.00	1.0000	0.0000	1.0000	0.0000

dos_mqtt_publish	1.00	1.00	1.0000	0.0000	1.0000	0.0000
dos_syn	1.00	1.00	1.0000	0.0000	1.0000	0.0000
dos_tcp	1.00	[illegible]	1.0000	0.0000	1.0000	0.0000
dos_udp	1.00	1.00	1.0000	0.0000	1.0000	0.0000
malformed_mqtt	0.98	0.98	0.9708	0.0000	1.0000	0.0292
os_scan	0.98	0.88	0.7916	0.0000	1.0000	0.2084
ping_sweep	1.00	0.99	0.9932	0.0000	1.0000	0.0068
port_scan	0.96	0.98	0.9962	0.0005	0.9995	0.0038
vul_scan	0.99	0.94	0.8946	0.0000	1.0000	0.1054

Tabel 4. 7 *Random Forest* 30 fitur data latih

Class	**Precision**	**F1-Score**	**FPR**	**TPR**	**FNR**	**TNR**
arp_spoofing	1.00	1.00	0.0000	0.9998	0.0002	1.0000
benign	1.00	1.00	0.0000	1.0000	0.0000	1.0000
ddos_icmp	1.00	1.00	0.0000	1.0000	0.0000	1.0000
ddos_mqtt_connect	1.00	1.00	0.0000	1.0000	0.0000	1.0000
ddos_mqtt_publish	1.00	1.00	0.0000	1.0000	0.0000	1.0000
ddos_syn	1.00	1.00	0.0000	1.0000	0.0000	1.0000
ddos_tcp	1.00	1.00	0.0000	1.0000	0.0000	1.0000
ddos_udp	1.00	1.00	0.0000	1.0000	0.0000	1.0000
dos_icmp	1.00	1.00	0.0000	1.0000	0.0000	1.0000
dos_mqtt_connect	1.00	1.00	0.0000	1.0000	0.0000	1.0000
dos_mqtt_publish	1.00	1.00	0.0000	1.0000	0.0000	1.0000
dos_syn	1.00	1.00	0.0000	1.0000	0.0000	1.0000
dos_tcp	1.00	1.00	0.0000	1.0000	0.0000	1.0000
dos_udp	1.00	1.00	0.0000	1.0000	0.0000	1.0000

malformed_mqtt	1.00	1.00	0.0000	0.9990	0.0010	1.0000
os_scan	0.99	0.93	0.0000	0.8856	0.1144	1.0000
ping_sweep	1.00	1.00	0.0000	0.9959	0.0041	1.0000
port_scan	0.98	0.99	0.0003	0.9972	0.0028	0.9997
vul_scan	0.99	0.97	0.0000	0.9531	0.0469	1.0000

Tabel 4. 8 *Random Forest* 40 fitur data latih

Class	Precision	F1-Score	FPR	TPR	FNR	TNR
arp_spoofing	1.00	1.00	0.0000	1.0000	0.0000	1.0000
benign	1.00	1.00	0.0000	1.0000	0.0000	1.0000
ddos_icmp	1.00	1.00	0.0000	1.0000	0.0000	1.0000
ddos_mqtt_connect	1.00	1.00	0.0000	1.0000	0.0000	1.0000
ddos_mqtt_publish	1.00	1.00	0.0000	1.0000	0.0000	1.0000
ddos_syn	1.00	1.00	0.0000	1.0000	0.0000	1.0000
ddos_tcp	1.00	1.00	0.0000	1.0000	0.0000	1.0000
ddos_udp	1.00	1.00	0.0000	1.0000	0.0000	1.0000
dos_icmp	1.00	1.00	0.0000	1.0000	0.0000	1.0000
dos_mqtt_connect	1.00	1.00	0.0000	1.0000	0.0000	1.0000
dos_mqtt_publish	1.00	1.00	0.0000	1.0000	0.0000	1.0000
dos_syn	1.00	1.00	0.0000	1.0000	0.0000	1.0000
dos_tcp	1.00	1.00	0.0000	1.0000	0.0000	1.0000
dos_udp	1.00	1.00	0.0000	1.0000	0.0000	1.0000
malformed_mqtt	1.00	1.00	0.0000	1.0000	0.0000	1.0000
os_scan	1.00	1.00	0.0000	0.9995	0.0005	1.0000
ping_sweep	1.00	1.00	0.0000	1.0000	0.0000	1.0000
port_scan	1.00	1.00	0.0000	1.0000	0.0000	1.0000

vul_scan	1.00	1.00	0.0000	1.0000	0.0000	1.0000

Tabel 4. 9 *Random Forest* Tanp[illegible]an fitur data latih

Class	Precision	F1-Score	FPR	TPR	FNR	TNR
arp_spoofing	1.00	1.00	0.0000	1.0000	0.0000	1.0000
benign	1.00	1.00	0.0000	1.0000	0.0000	1.0000
ddos_icmp	1.00	1.00	0.0000	1.0000	0.0000	1.0000
ddos_mqtt_connect	1.00	1.00	0.0000	1.0000	0.0000	1.0000
ddos_mqtt_publish	1.00	1.00	0.0000	1.0000	0.0000	1.0000
ddos_syn	1.00	1.00	0.0000	1.0000	0.0000	1.0000
ddos_tcp	1.00	1.00	0.0000	1.0000	0.0000	1.0000
ddos_udp	1.00	1.00	0.0000	1.0000	0.0000	1.0000
dos_icmp	1.00	1.00	0.0000	1.0000	0.0000	1.0000
dos_mqtt_connect	1.00	1.00	0.0000	1.0000	0.0000	1.0000
dos_mqtt_publish	1.00	1.00	0.0000	1.0000	0.0000	1.0000
dos_syn	1.00	1.00	0.0000	1.0000	0.0000	1.0000
dos_tcp	1.00	1.00	0.0000	1.0000	0.0000	1.0000
dos_udp	1.00	1.00	0.0000	1.0000	0.0000	1.0000
malformed_mqtt	1.00	1.00	0.0000	1.0000	0.0000	1.0000
os_scan	1.00	1.00	0.0000	0.9995	0.0005	1.0000
ping_sweep	1.00	1.00	0.0000	1.0000	0.0000	1.0000
port_scan	1.00	1.00	0.0000	1.0000	0.0000	1.0000
vul_scan	1.00	1.00	0.0000	1.0000	0.0000	1.0000

Tabel 4.10 sampai Tabel 4.14 menunjukkan kinerja model *machine learning* menggunakan algoritma *Rando* [illegible] *t* pada data uji.

Tabel 4. 10 *Random Forest* 10 [illegible] uji

Class	**Precision**	**F1-Score**	**FPR**	**TPR**	**FNR**	**TNR**
arp_spoofing	0.58	0.61	0.0005	0.6537	0.3463	0.9995
benign	0.96	0.97	0.0009	0.9741	0.0259	0.9991
ddos_icmp	1.00	1.00	0.0002	1.0000	0.0000	0.9998
ddos_mqtt_connect	1.00	1.00	0.0000	1.0000	0.0000	1.0000
ddos_mqtt_publish	1.00	1.00	0.0000	0.9922	0.0078	1.0000
ddos_syn	1.00	1.00	0.0000	0.9989	0.0011	1.0000
ddos_tcp	1.00	1.00	0.0000	1.0000	0.0000	1.0000
ddos_udp	1.00	1.00	0.0001	0.9995	0.0005	0.9999
dos_icmp	0.97	0.99	0.0018	0.9998	0.0002	0.9982
dos_mqtt_connect	1.00	1.00	0.0000	0.9990	0.0010	1.0000
dos_mqtt_publish	1.00	1.00	0.0000	1.0000	0.0000	1.0000
dos_syn	1.00	1.00	0.0000	0.9995	0.0005	1.0000
dos_tcp	1.00	1.00	0.0000	0.9998	0.0002	1.0000
dos_udp	1.00	0.99	0.0000	0.9801	0.0199	1.0000
malformed_mqtt	0.98	0.85	0.0000	0.7584	0.2416	1.0000
os_scan	0.80	0.66	0.0003	0.5642	0.4358	0.9997
ping_sweep	0.60	0.66	0.0001	0.7366	0.2634	0.9999
port_scan	0.92	0.95	0.0012	0.9696	0.0304	0.9988
vul_scan	0.72	0.54	0.0001	0.4362	0.5638	0.9999

Tabel 4. 11 *Random Forest* 20 fitur data uji

Class	Precisi	F1- re	FPR	TPR	FNR	TNR
arp_spoofing	0.96	[illegible]	0.0000	0.5069	0.4931	1.0000
benign	0.93	0.96	0.0018	0.9930	0.0070	0.9982
ddos_icmp	0.73	0.84	0.1042	1.0000	0.0000	0.8958
ddos_mqtt_connect	1.00	1.00	0.0000	0.9996	0.0004	1.0000
ddos_mqtt_publish	1.00	0.83	0.0000	0.7043	0.2957	1.0000
ddos_syn	1.00	1.00	0.0000	0.9984	0.0016	1.0000
ddos_tcp	1.00	1.00	0.0000	0.9992	0.0008	1.0000
ddos_udp	1.00	0.78	0.0002	0.6369	0.3631	0.9998
dos_icmp	0.41	0.58	0.0924	0.9997	0.0003	0.9076
dos_mqtt_connect	1.00	1.00	0.0000	0.9978	0.0022	1.0000
dos_mqtt_publish	1.00	0.84	0.0000	0.7267	0.2733	1.0000
dos_syn	1.00	1.00	0.0000	0.9995	0.0005	1.0000
dos_tcp	1.00	0.99	0.0000	0.9888	0.0112	1.0000
dos_udp	1.00	0.05	0.0000	0.0246	0.9754	1.0000
malformed_mqtt	1.00	0.76	0.0000	0.6176	0.3824	1.0000
os_scan	0.74	0.64	0.0005	0.5574	0.4426	0.9995
ping_sweep	0.60	0.61	0.0000	0.6290	0.3710	1.0000
port_scan	0.93	0.94	0.0010	0.9499	0.0501	0.9990
vul_scan	0.94	0.35	0.0000	0.2137	0.7863	1.0000

Tabel 4. 12 *Random Forest* 30 fitur data uji

Class	**Precisi**	**F1- re**	**FPR**	**TPR**	**FNR**	**TNR**
arp_spoofing	0.46	[illegible]9	0.0010	0.8114	0.1886	0.9990
benign	0.97	0.96	0.0008	0.9596	0.0404	0.9992
ddos_icmp	1.00	1.00	0.0001	0.9998	0.0002	0.9999
ddos_mqtt_connect	1.00	1.00	0.0000	1.0000	0.0000	1.0000
ddos_mqtt_publish	1.00	0.99	0.0000	0.9761	0.0239	1.0000
ddos_syn	1.00	1.00	0.0000	0.9984	0.0016	1.0000
ddos_tcp	1.00	1.00	0.0000	1.0000	0.0000	1.0000
ddos_udp	1.00	1.00	0.0003	0.9996	0.0004	0.9997
dos_icmp	1.00	1.00	0.0000	0.9996	0.0004	1.0000
dos_mqtt_connect	1.00	1.00	0.0000	0.9990	0.0010	1.0000
dos_mqtt_publish	0.98	0.99	0.0001	1.0000	0.0000	0.9999
dos_syn	1.00	1.00	0.0000	0.9999	0.0001	1.0000
dos_tcp	1.00	1.00	0.0000	0.9999	0.0001	1.0000
dos_udp	1.00	1.00	0.0000	0.9994	0.0006	1.0000
malformed_mqtt	1.00	0.88	0.0000	0.7934	0.2066	1.0000
os_scan	0.75	0.64	0.0005	0.5670	0.4330	0.9995
ping_sweep	0.88	0.81	0.0000	0.7419	0.2581	1.0000
port_scan	0.93	0.95	0.0010	0.9696	0.0304	0.9990
vul_scan	0.79	0.43	0.0000	0.2921	0.7079	1.0000

Tabel 4. 13 *Random Forest* 40 fitur data uji

Class	Precisi	F1- re	FPR	TPR	FNR	TNR
arp_spoofing	0.78	[illegible]	0.0003	0.4987	0.5013	0.9997
benign	0.97	0.96	0.0009	0.9608	0.0392	0.9991
ddos_icmp	1.00	1.00	0.0000	0.9995	0.0005	1.0000
ddos_mqtt_connect	1.00	1.00	0.0000	0.9980	0.0020	1.0000
ddos_mqtt_publish	0.98	0.99	0.0001	0.9935	0.0065	0.9999
ddos_syn	0.99	1.00	0.0008	0.9995	0.0005	0.9992
ddos_tcp	1.00	1.00	0.0000	0.9970	0.0030	1.0000
ddos_udp	1.00	1.00	0.0002	0.9980	0.0020	0.9998
dos_icmp	1.00	1.00	0.0002	0.9984	0.0016	0.9998
dos_mqtt_connect	1.00	0.99	0.0000	0.9888	0.0112	1.0000
dos_mqtt_publish	1.00	1.00	0.0000	0.9974	0.0026	1.0000
dos_syn	1.00	1.00	0.0001	0.9929	0.0071	0.9999
dos_tcp	1.00	1.00	0.0000	0.9988	0.0012	1.0000
dos_udp	0.99	1.00	0.0005	0.9973	0.0027	0.9995
malformed_mqtt	0.32	0.47	0.0014	0.9261	0.0739	0.9986
os_scan	0.68	0.68	0.0008	0.6760	0.3240	0.9992
ping_sweep	0.62	0.69	0.0000	0.7676	0.2324	1.0000
port_scan	0.93	0.92	0.0008	0.9020	0.0980	0.9992
vul_scan	0.35	0.38	0.0002	0.4234	0.5766	0.9998

Tabel 4. 14 *Random Forest* Tanpa pemilihan fitur data uji

Class	Precisi	F1- re	FPR	TPR	FNR	TNR
arp_spoofing	0.71	7	0.0004	0.4798	0.5202	0.9996
benign	0.97	0.97	0.0009	0.9645	0.0355	0.9991
ddos_icmp	1.00	1.00	0.0000	0.9996	0.0004	1.0000
ddos_mqtt_connect	1.00	1.00	0.0000	0.9976	0.0024	1.0000
ddos_mqtt_publish	0.98	0.99	0.0001	0.9927	0.0073	0.9999
ddos_syn	0.99	1.00	0.0011	0.9994	0.0006	0.9989
ddos_tcp	1.00	1.00	0.0000	0.9968	0.0032	1.0000
ddos_udp	1.00	1.00	0.0002	0.9991	0.0009	0.9998
dos_icmp	1.00	1.00	0.0002	0.9987	0.0013	0.9998
dos_mqtt_connect	1.00	0.99	0.0000	0.9939	0.0061	1.0000
dos_mqtt_publish	1.00	1.00	0.0000	0.9979	0.0021	1.0000
dos_syn	1.00	0.99	0.0001	0.9897	0.0103	0.9999
dos_tcp	1.00	1.00	0.0001	0.9989	0.0011	0.9999
dos_udp	1.00	1.00	0.0002	0.9973	0.0027	0.9998
malformed_mqtt	0.33	0.49	0.0014	0.9302	0.0698	0.9986
os_scan	0.64	0.66	0.0009	0.6747	0.3253	0.9991
ping_sweep	0.62	0.68	0.0000	0.7595	0.2405	1.0000
port_scan	0.93	0.91	0.0008	0.8882	0.1118	0.9992
vul_scan	0.31	0.32	0.0002	0.3254	0.6746	0.9998

Tabel 4.15 dan tabel 4.16 menunjukkan kinerja model *machine learning* menggunakan algoritma *gradie*[illegible]*ting* pada data latih dan data uji.

Tabel 4. 15 *Gradient Boosting* [illegible]ilihan fitur data latih

Class	Prec	F1	TPR	FPR	FNR	TNR
benign	0.97	0.98	0.98	0.00	0.02	0.99
arp_spoofing	0.80	0.79	0.78	0.00	0.22	0.99
ddos_mqtt_connect	1.00	1.00	1.00	0.00	0.00	1.00
ddos_mqtt_publish	1.00	1.00	1.00	0.00	0.00	1.00
dos_mqtt_connect	1.00	1.00	1.00	0.00	0.00	1.00
dos_mqtt_publish	0.99	1.00	1.00	0.00	0.00	1.00
malformed_mqtt	0.85	0.80	0.76	0.00	0.24	0.99
os_scan	0.87	0.68	0.55	0.00	0.45	0.99
ping_sweep	0.68	0.47	0.35	0.00	0.65	0.99
port_scan	0.91	0.94	0.94	0.00	0.04	0.99
vul_scan	0.67	0.56	0.48	0.00	0.52	0.99
ddos_icmp	1.00	1.00	1.00	0.00	0.00	1.00
ddos_syn	1.00	1.00	1.00	0.00	0.00	1.00
ddos_tcp	1.00	1.00	1.00	0.00	0.00	1.00
ddos_udp	1.00	1.00	1.00	0.00	0.00	1.00
dos_icmp	1.00	1.00	1.00	0.00	0.00	1.00
dos_syn	1.00	1.00	1.00	0.00	0.00	1.00
dos_tcp	1.00	1.00	1.00	0.00	0.00	1.00
dos_udp	1.00	1.00	1.00	0.00	0.00	1.00

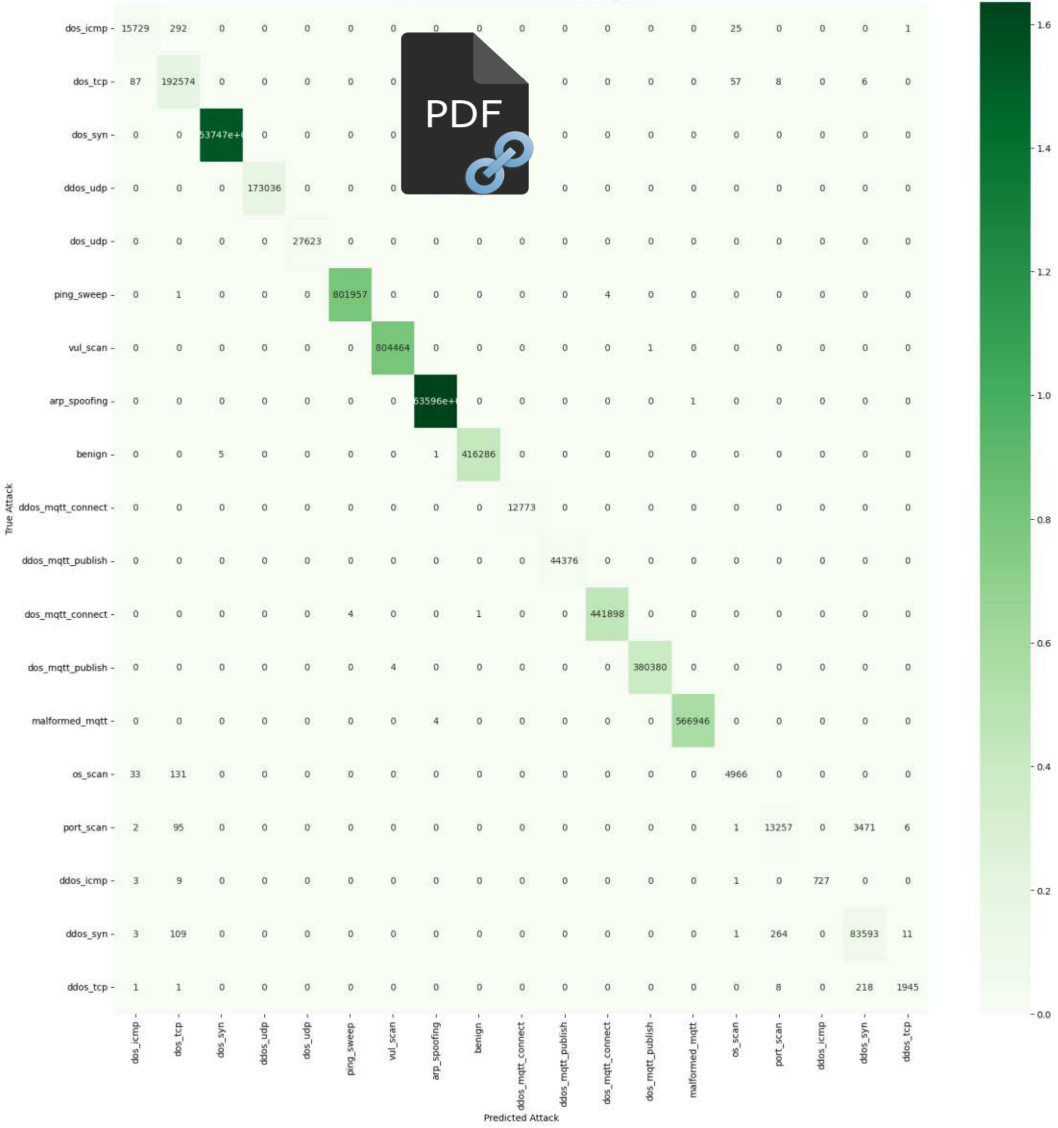
Tabel 4. 16 *Gradient Boosting* Tanpa pemilihan fitur data uji

Class	Prec	F1	TPR	FPR	FNR	TNR
benign	0.96	0.96	0.97	0.00	0.03	0.99
arp_spoofing	0.46	0.56	0.72	0.00	0.28	0.99
ddos_mqtt_connect	1.00	1.00	1.00	0.00	0.00	1.00
ddos_mqtt_publish	1.00	0.93	0.87	0.00	0.13	1.00
dos_mqtt_connect	1.00	1.00	1.00	0.00	0.00	1.00
dos_mqtt_publish	0.89	0.94	1.00	0.00	0.00	1.00
malformed_mqtt	0.92	0.82	0.74	0.00	0.26	0.99
os_scan	0.83	0.87	0.57	0.00	0.43	0.99
ping_sweep	0.43	0.45	0.43	0.00	0.57	0.99

port_scan	0.92	0.95	0.97	0.00	0.03	0.99
vul_scan	0.58	[illegible]	[illegible]	0.00	0.75	0.99
ddos_icmp	0.60	[illegible]	[illegible]	0.12	0.00	0.88
ddos_syn	1.00	1.00	1.00	0.00	0.00	1.00
ddos_tcp	1.00	1.00	1.00	0.00	0.00	1.00
ddos_udp	0.99	0.29	0.17	0.00	0.83	1.00
dos_icmp	0.42	0.59	0.99	0.12	0.00	0.88
dos_syn	1.00	1.00	1.00	0.00	0.00	1.00
dos_tcp	1.00	1.00	1.00	0.00	0.00	1.00
dos_udp	1.00	0.05	0.02	0.00	0.98	1.00

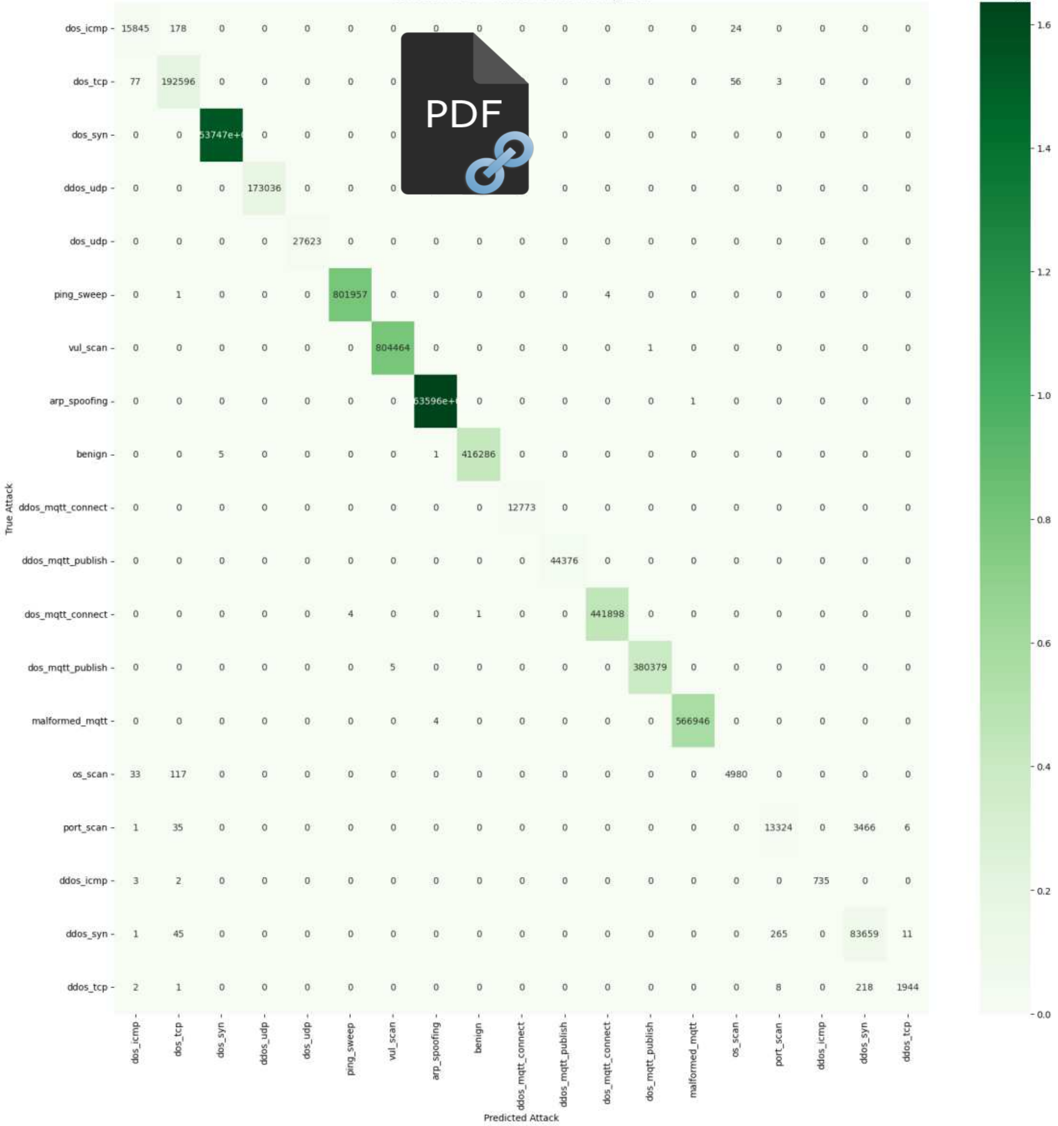
Berdasarkan evaluasi kinerja model *machine learning* pada data pelatihan, algoritma *Random Forest* dan *Gradient Boosting* menunjukkan hasil yang sangat baik dengan kinerja sempurna di semua kelas. Nilai *precision*, *f1-score*, *True Positive Rate (TPR), False Positive Rate (FPR), False Negative Rate (FNR),* dan *True Negative Rate (TNR)* hampir mencapai 100 %. Hasil ini mengindikasikan bahwa model mampu mendeteksi semua jenis serangan secara akurat, sehingga membuktikan efektivitas kedua algoritma dalam mengidentifikasi ancaman pada jaringan.

Kinerja setiap model yang dilatih menggunakan data latih dan data uji dalam penelitian ini divisualisasikan melalui *confusion matrix*. Gambar 4.3 menampilkan *confusion matrix* untuk algoritma *Random Forest,* yang menggambarkan kemampuan model dalam mengklasifikasikan titik data, baik yang termasuk kategori normal maupun serangan, dengan akurasi yang tinggi. Hal ini mencerminkan efektivitas algoritma *Random Forest* dalam menangani klasifikasi secara tepat.

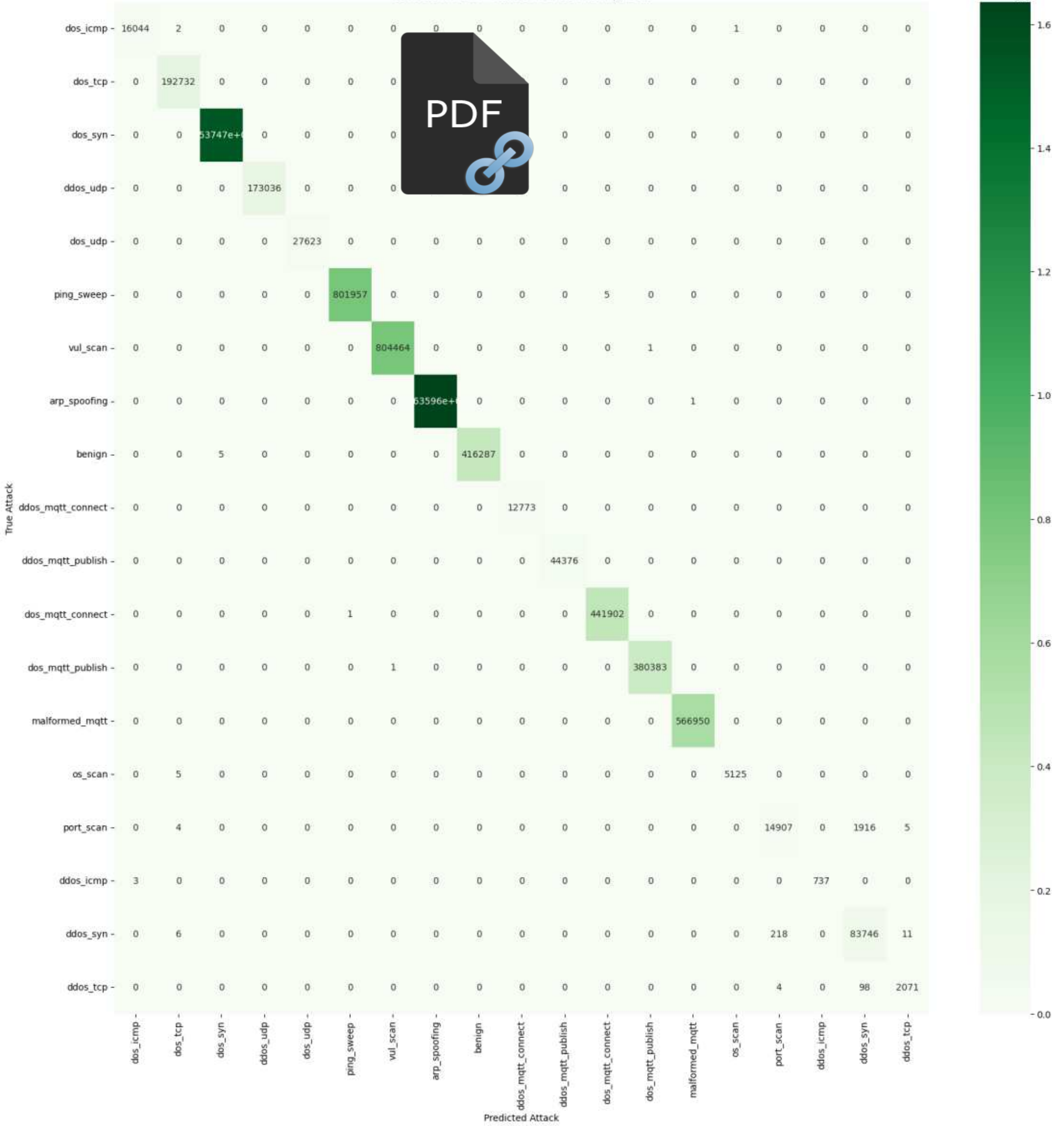


	dos_icmp	dos_tcp	dos_syn	ddos_udp	dos_udp	ping_sweep	vul_scan	arp_spoofing	benign	ddos_mqtt_connect	ddos_mqtt_publish	dos_mqtt_connect	dos_mqtt_publish	malformed_mqtt	os_scan	port_scan	ddos_icmp	ddos_syn	ddos_tcp
dos_icmp	15729	292	0	0	0	0	0	0	0	0	0	0	0	0	25	0	0	0	1
dos_tcp	87	192574	0	0	0	0	0	[illegible]	[illegible]	[illegible]	0	0	0	0	57	8	0	6	0
dos_syn	0	0	53747e+	0	0	0	0	[illegible]	[illegible]	[illegible]	0	0	0	0	0	0	0	0	0
ddos_udp	0	0	0	173036	0	0	0	[illegible]	[illegible]	[illegible]	0	0	0	0	0	0	0	0	0
dos_udp	0	0	0	0	27623	0	0	0	0	0	0	0	0	0	0	0	0	0	0
ping_sweep	0	1	0	0	0	801957	0	0	0	0	0	4	0	0	0	0	0	0	0
vul_scan	0	0	0	0	0	0	804464	0	0	0	0	0	1	0	0	0	0	0	0
arp_spoofing	0	0	0	0	0	0	0	63596e+	0	0	0	0	0	1	0	0	0	0	0
benign	0	0	5	0	0	0	0	1	416286	0	0	0	0	0	0	0	0	0	0
ddos_mqtt_connect	0	0	0	0	0	0	0	0	0	12773	0	0	0	0	0	0	0	0	0
ddos_mqtt_publish	0	0	0	0	0	0	0	0	0	0	44376	0	0	0	0	0	0	0	0
dos_mqtt_connect	0	0	0	0	0	4	0	0	1	0	0	441898	0	0	0	0	0	0	0
dos_mqtt_publish	0	0	0	0	0	0	4	0	0	0	0	0	380380	0	0	0	0	0	0
malformed_mqtt	0	0	0	0	0	0	0	4	0	0	0	0	0	566946	0	0	0	0	0
os_scan	33	131	0	0	0	0	0	0	0	0	0	0	0	0	4966	0	0	0	0
port_scan	2	95	0	0	0	0	0	0	0	0	0	0	0	0	1	13257	0	3471	6
ddos_icmp	3	9	0	0	0	0	0	0	0	0	0	0	0	0	1	0	727	0	0
ddos_syn	3	109	0	0	0	0	0	0	0	0	0	0	0	0	1	264	0	83593	11
ddos_tcp	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	8	0	218	1945

Gambar 4. 3 *Confusion Matrix* RF 10 Fitur data latih

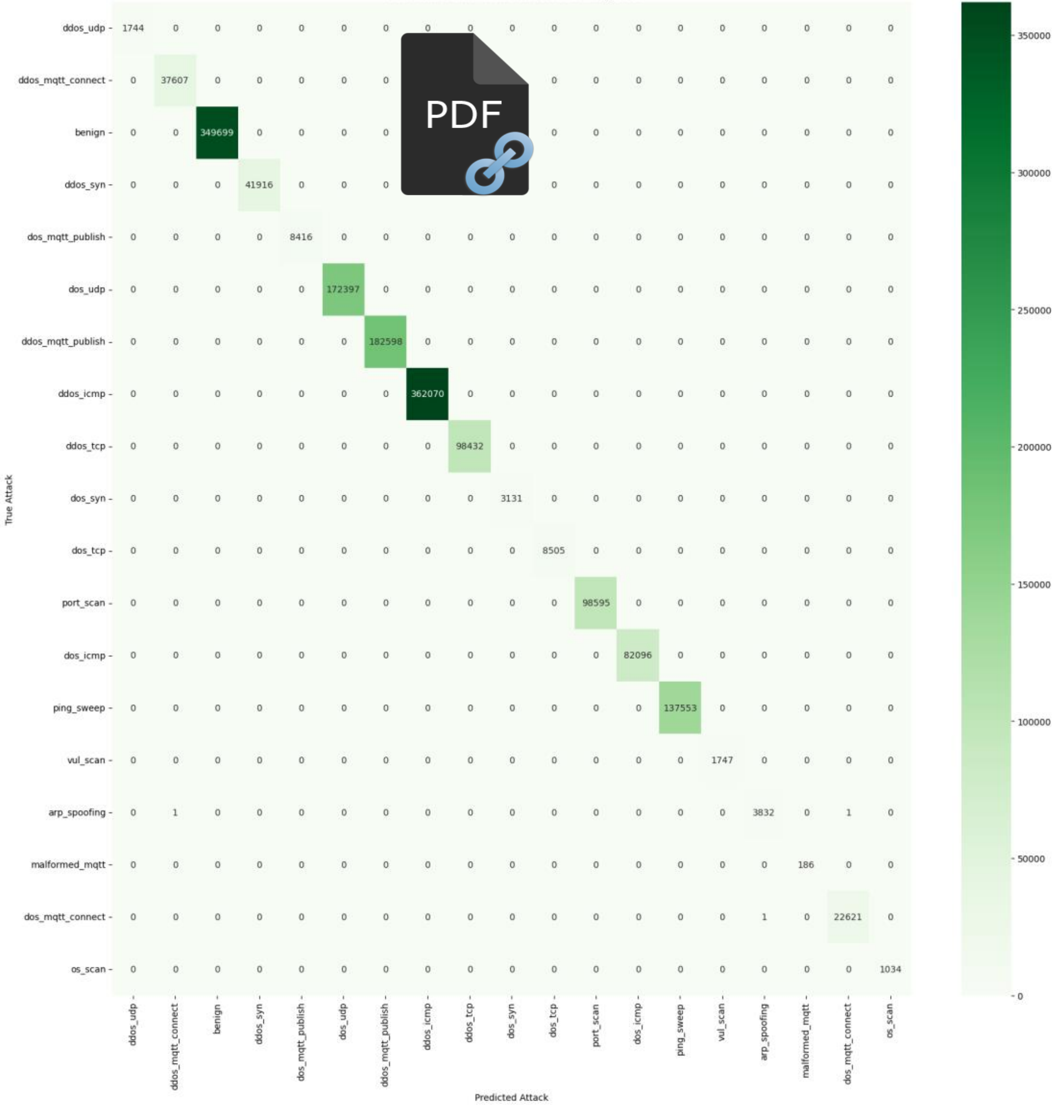


Gambar 4. 4 *Confusion Matrix* RF 20 Fitur data latih



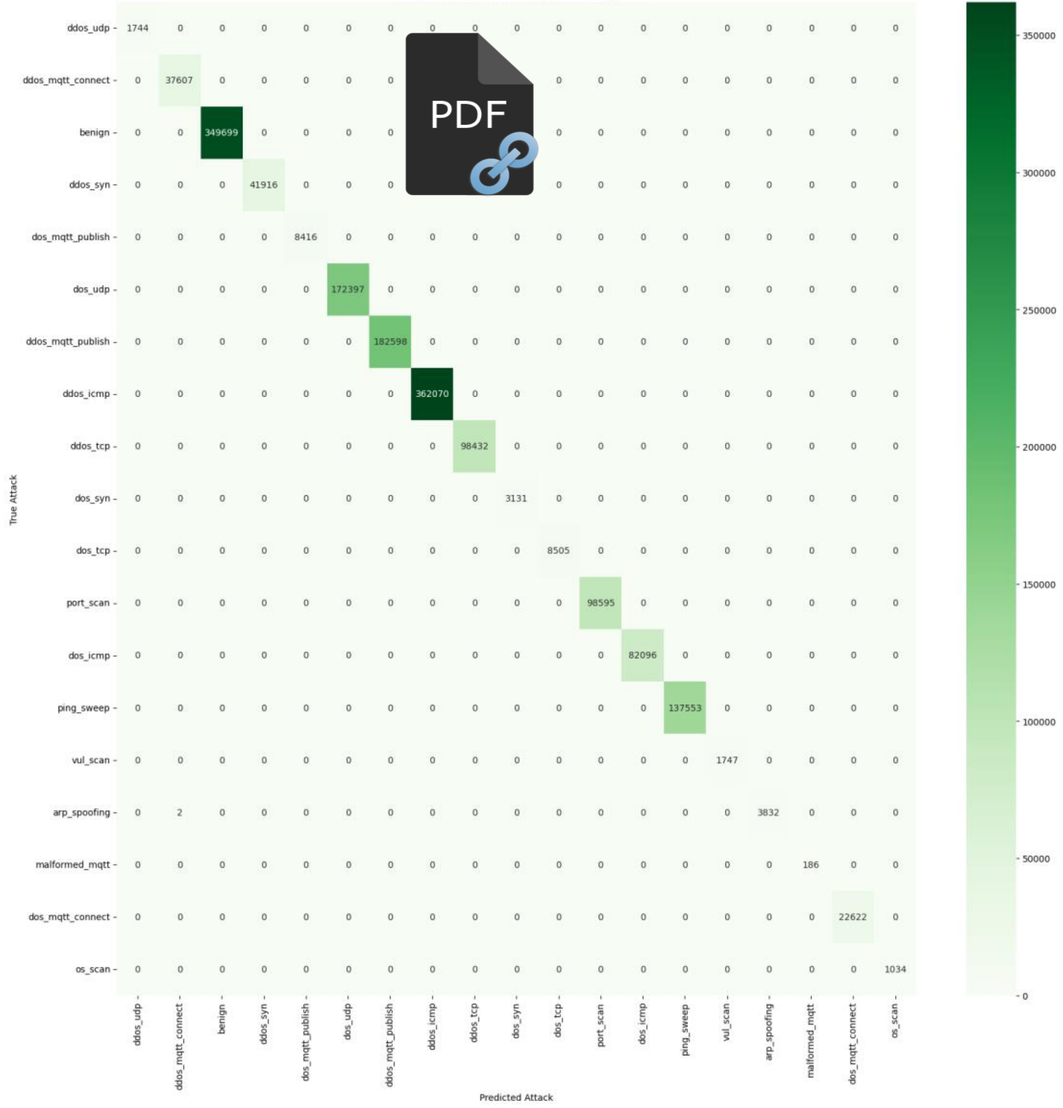
	dos_icmp	dos_tcp	dos_syn	ddos_udp	dos_udp	ping_sweep	vul_scan	arp_spoofing	benign	ddos_mqtt_connect	ddos_mqtt_publish	dos_mqtt_connect	dos_mqtt_publish	malformed_mqtt	os_scan	port_scan	ddos_icmp	ddos_syn	ddos_tcp
dos_icmp	16044	2	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0
dos_tcp	0	192732	0	0	0	0	0	[illegible]	[illegible]	[illegible]	0	0	0	0	0	0	0	0	0
dos_syn	0	0	53747e+	0	0	0	0	[illegible]	[illegible]	[illegible]	0	0	0	0	0	0	0	0	0
ddos_udp	0	0	0	173036	0	0	0	[illegible]	[illegible]	[illegible]	0	0	0	0	0	0	0	0	0
dos_udp	0	0	0	0	27623	0	0	0	0	0	0	0	0	0	0	0	0	0	0
ping_sweep	0	0	0	0	0	801957	0	0	0	0	0	5	0	0	0	0	0	0	0
vul_scan	0	0	0	0	0	0	804464	0	0	0	0	0	1	0	0	0	0	0	0
arp_spoofing	0	0	0	0	0	0	0	63596e+	0	0	0	0	0	1	0	0	0	0	0
benign	0	0	5	0	0	0	0	0	416287	0	0	0	0	0	0	0	0	0	0
ddos_mqtt_connect	0	0	0	0	0	0	0	0	0	12773	0	0	0	0	0	0	0	0	0
ddos_mqtt_publish	0	0	0	0	0	0	0	0	0	0	44376	0	0	0	0	0	0	0	0
dos_mqtt_connect	0	0	0	0	0	1	0	0	0	0	0	441902	0	0	0	0	0	0	0
dos_mqtt_publish	0	0	0	0	0	0	1	0	0	0	0	0	380383	0	0	0	0	0	0
malformed_mqtt	0	0	0	0	0	0	0	0	0	0	0	0	0	566950	0	0	0	0	0
os_scan	0	5	0	0	0	0	0	0	0	0	0	0	0	0	5125	0	0	0	0
port_scan	0	4	0	0	0	0	0	0	0	0	0	0	0	0	0	14907	0	1916	5
ddos_icmp	3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	737	0	0
ddos_syn	0	6	0	0	0	0	0	0	0	0	0	0	0	0	0	218	0	83746	11
ddos_tcp	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	4	0	98	2071

Gambar 4. 5 *Confusion Matrix* RF 30 Fitur data latih



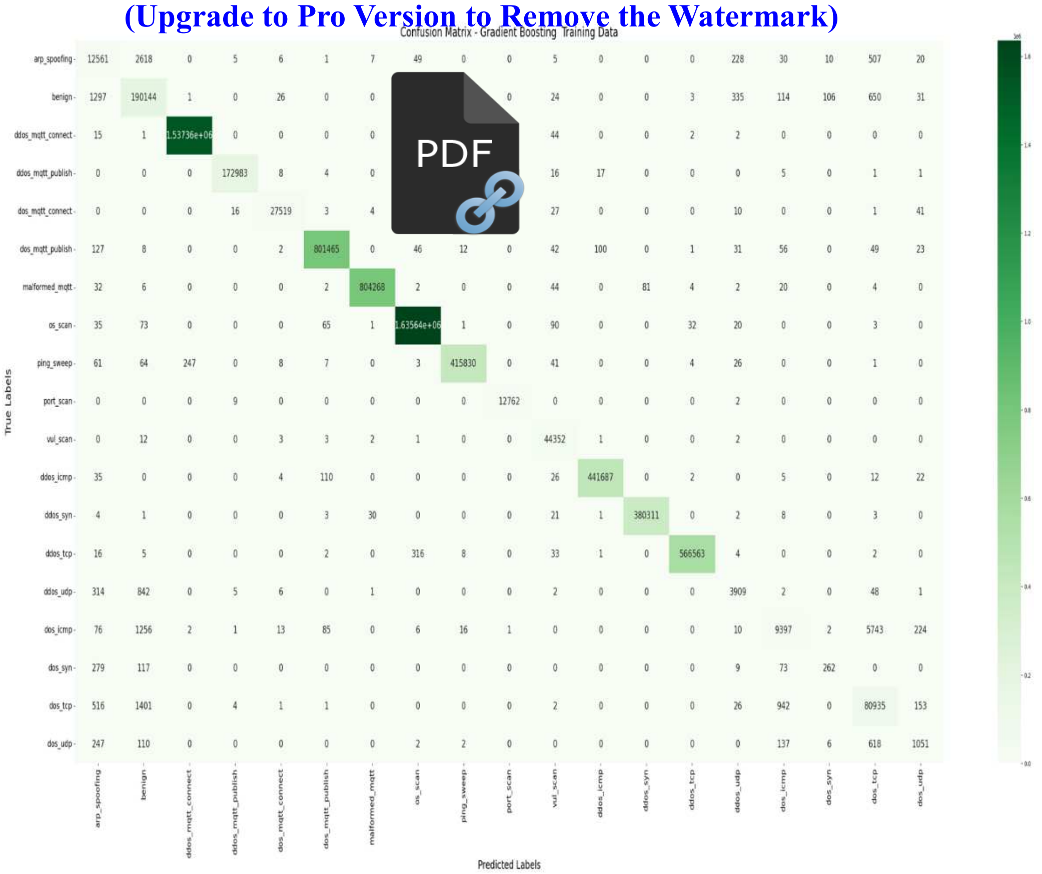
	ddos_udp	ddos_mqtt_connect	benign	ddos_syn	dos_mqtt_publish	dos_udp	ddos_mqtt_publish	ddos_icmp	ddos_tcp	dos_syn	dos_tcp	port_scan	dos_icmp	ping_sweep	vul_scan	arp_spoofing	malformed_mqtt	dos_mqtt_connect	os_scan
ddos_udp	1744	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
ddos_mqtt_connect	0	37607	0	0	0	0	0	[illegible]	[illegible]	[illegible]	0	0	0	0	0	0	0	0	0
benign	0	0	349699	0	0	0	0	[illegible]	[illegible]	[illegible]	0	0	0	0	0	0	0	0	0
ddos_syn	0	0	0	41916	0	0	0	[illegible]	[illegible]	[illegible]	0	0	0	0	0	0	0	0	0
dos_mqtt_publish	0	0	0	0	8416	0	0	0	0	0	0	0	0	0	0	0	0	0	0
dos_udp	0	0	0	0	0	172397	0	0	0	0	0	0	0	0	0	0	0	0	0
ddos_mqtt_publish	0	0	0	0	0	0	182598	0	0	0	0	0	0	0	0	0	0	0	0
ddos_icmp	0	0	0	0	0	0	0	362070	0	0	0	0	0	0	0	0	0	0	0
ddos_tcp	0	0	0	0	0	0	0	0	98432	0	0	0	0	0	0	0	0	0	0
dos_syn	0	0	0	0	0	0	0	0	0	3131	0	0	0	0	0	0	0	0	0
dos_tcp	0	0	0	0	0	0	0	0	0	0	8505	0	0	0	0	0	0	0	0
port_scan	0	0	0	0	0	0	0	0	0	0	0	98595	0	0	0	0	0	0	0
dos_icmp	0	0	0	0	0	0	0	0	0	0	0	0	82096	0	0	0	0	0	0
ping_sweep	0	0	0	0	0	0	0	0	0	0	0	0	0	137553	0	0	0	0	0
vul_scan	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1747	0	0	0	0
arp_spoofing	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	3832	0	1	0
malformed_mqtt	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	186	0	0
dos_mqtt_connect	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	22621	0
os_scan	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1034

Gambar 4. 6 *Confusion Matrix* RF 40 Fitur data latih



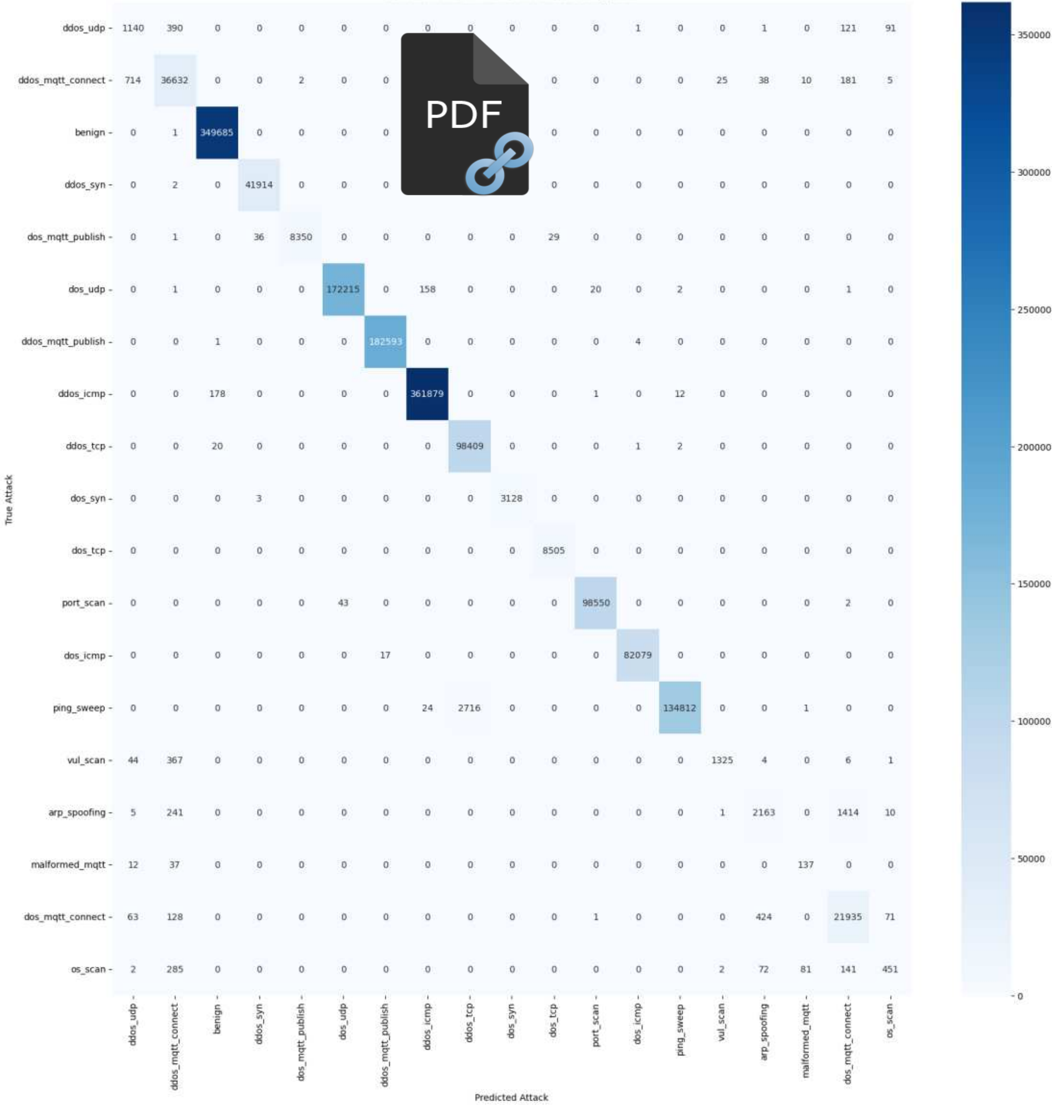
	ddos_udp	ddos_mqtt_connect	benign	ddos_syn	dos_mqtt_publish	dos_udp	ddos_mqtt_publish	ddos_icmp	ddos_tcp	dos_syn	dos_tcp	port_scan	dos_icmp	ping_sweep	vul_scan	arp_spoofing	malformed_mqtt	dos_mqtt_connect	os_scan
ddos_udp	1744	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
ddos_mqtt_connect	0	37607	0	0	0	0	0	[illegible]	[illegible]	[illegible]	0	0	0	0	0	0	0	0	0
benign	0	0	349699	0	0	0	0	[illegible]	[illegible]	[illegible]	0	0	0	0	0	0	0	0	0
ddos_syn	0	0	0	41916	0	0	0	[illegible]	[illegible]	[illegible]	0	0	0	0	0	0	0	0	0
dos_mqtt_publish	0	0	0	0	8416	0	0	0	0	0	0	0	0	0	0	0	0	0	0
dos_udp	0	0	0	0	0	172397	0	0	0	0	0	0	0	0	0	0	0	0	0
ddos_mqtt_publish	0	0	0	0	0	0	182598	0	0	0	0	0	0	0	0	0	0	0	0
ddos_icmp	0	0	0	0	0	0	0	362070	0	0	0	0	0	0	0	0	0	0	0
ddos_tcp	0	0	0	0	0	0	0	0	98432	0	0	0	0	0	0	0	0	0	0
dos_syn	0	0	0	0	0	0	0	0	0	3131	0	0	0	0	0	0	0	0	0
dos_tcp	0	0	0	0	0	0	0	0	0	0	8505	0	0	0	0	0	0	0	0
port_scan	0	0	0	0	0	0	0	0	0	0	0	98595	0	0	0	0	0	0	0
dos_icmp	0	0	0	0	0	0	0	0	0	0	0	0	82096	0	0	0	0	0	0
ping_sweep	0	0	0	0	0	0	0	0	0	0	0	0	0	137553	0	0	0	0	0
vul_scan	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1747	0	0	0	0
arp_spoofing	0	2	0	0	0	0	0	0	0	0	0	0	0	0	0	3832	0	0	0
malformed_mqtt	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	186	0	0
dos_mqtt_connect	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	22622	0
os_scan	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1034

Gambar 4. 7 *Confusion Matrix* RF Tanpa pemilihan Fitur data latih



	arp_spoofing	benign	ddos_mqtt_connect	ddos_mqtt_publish	dos_mqtt_connect	dos_mqtt_publish	malformed_mqtt	os_scan	ping_sweep	port_scan	vul_scan	ddos_icmp	ddos_syn	ddos_tcp	ddos_udp	dos_icmp	dos_syn	dos_tcp	dos_udp
arp_spoofing	12561	2618	0	5	6	1	7	49	0	0	5	0	0	0	228	30	10	507	20
benign	1297	190144	1	0	26	0	0	[illegible]	[illegible]	0	24	0	0	3	335	114	106	650	31
ddos_mqtt_connect	15	1	1.53736e+06	0	0	0	0	[illegible]	[illegible]	[illegible]	44	0	0	2	2	0	0	0	0
ddos_mqtt_publish	0	0	0	172983	8	4	0	[illegible]	[illegible]	[illegible]	16	17	0	0	0	5	0	1	1
dos_mqtt_connect	0	0	0	16	27519	3	4	[illegible]	[illegible]	[illegible]	27	0	0	0	10	0	0	1	41
dos_mqtt_publish	127	8	0	0	2	801465	0	46	12	0	42	100	0	1	31	56	0	49	23
malformed_mqtt	32	6	0	0	0	2	804268	2	0	0	44	0	81	4	2	20	0	4	0
os_scan	35	73	0	0	0	65	1	1.63564e+06	1	0	90	0	0	32	20	0	0	3	0
ping_sweep	61	64	247	0	8	7	0	3	415830	0	41	0	0	4	26	0	0	1	0
port_scan	0	0	0	9	0	0	0	0	0	12762	0	0	0	0	2	0	0	0	0
vul_scan	0	12	0	0	3	3	2	1	0	0	44352	1	0	0	2	0	0	0	0
ddos_icmp	35	0	0	0	4	110	0	0	0	0	26	441687	0	2	0	5	0	12	22
ddos_syn	4	1	0	0	0	3	30	0	0	0	21	1	380311	0	2	8	0	3	0
ddos_tcp	16	5	0	0	0	2	0	316	8	0	33	1	0	566563	4	0	0	2	0
ddos_udp	314	842	0	5	6	0	1	0	0	0	2	0	0	0	3909	2	0	48	1
dos_icmp	76	1256	2	1	13	85	0	6	16	1	0	0	0	0	10	9397	2	5743	224
dos_syn	279	117	0	0	0	0	0	0	0	0	0	0	0	0	9	73	262	0	0
dos_tcp	516	1401	0	4	1	1	0	0	0	0	2	0	0	0	26	942	0	80935	153
dos_udp	247	110	0	0	0	0	0	2	2	0	0	0	0	0	0	137	6	618	1051

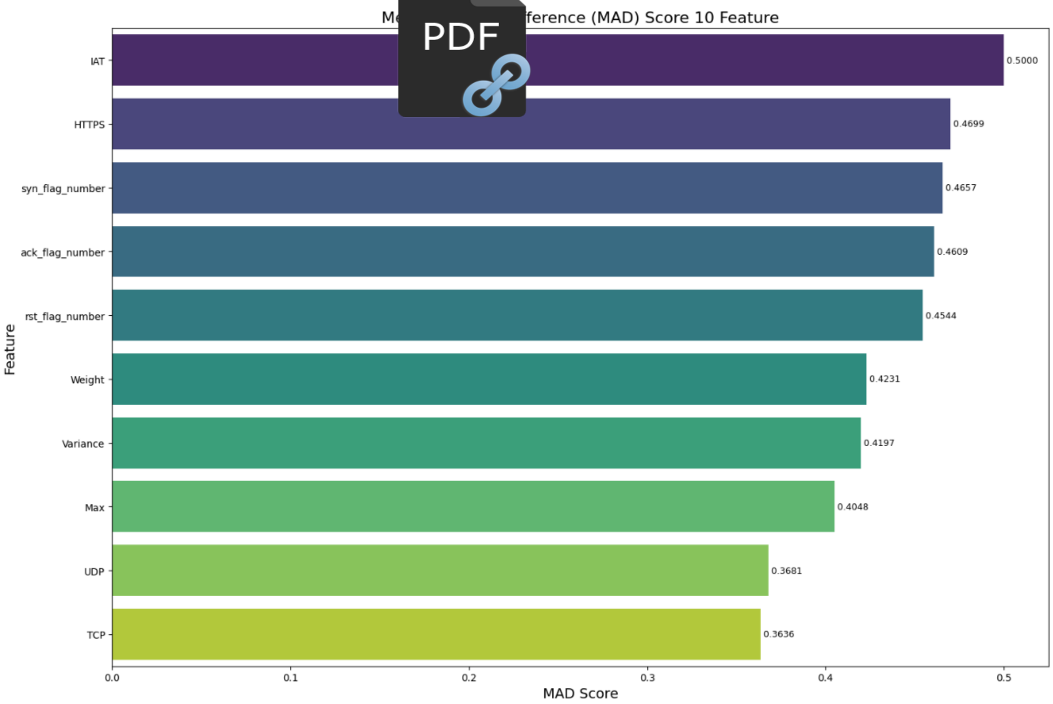
Gambar 4. 8 *Confusion Matrix* GB Tanpa pemilihan Fitur data latih



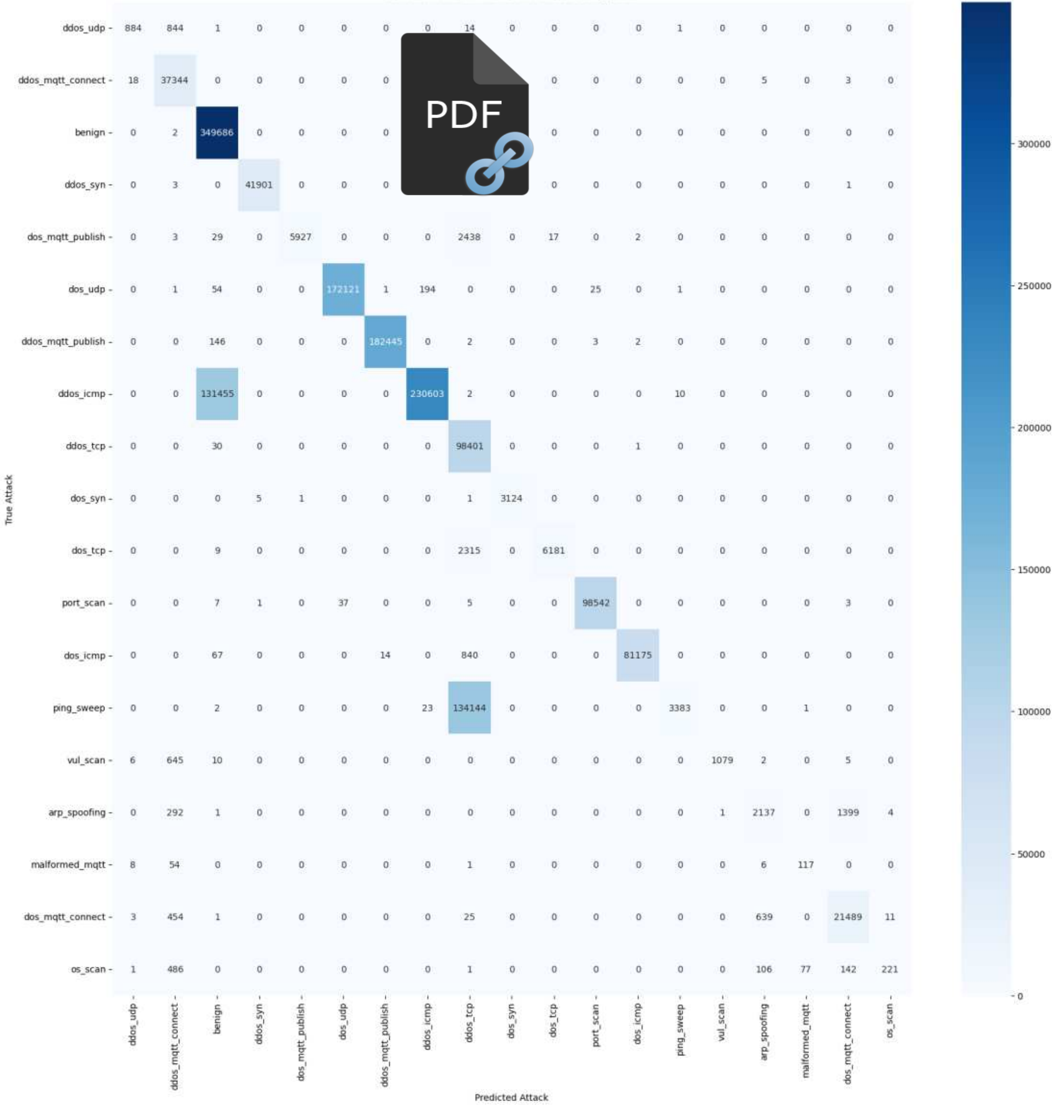
	ddos_udp	ddos_mqtt_connect	benign	ddos_syn	dos_mqtt_publish	dos_udp	ddos_mqtt_publish	ddos_icmp	ddos_tcp	dos_syn	dos_tcp	port_scan	dos_icmp	ping_sweep	vul_scan	arp_spoofing	malformed_mqtt	dos_mqtt_connect	os_scan
ddos_udp	1140	390	0	0	0	0	0	0	0	0	0	0	1	0	0	1	0	121	91
ddos_mqtt_connect	714	36632	0	0	2	0	0	[illegible]	[illegible]	[illegible]	0	0	0	0	25	38	10	181	5
benign	0	1	349685	0	0	0	0	[illegible]	[illegible]	[illegible]	0	0	0	0	0	0	0	0	0
ddos_syn	0	2	0	41914	0	0	0	[illegible]	[illegible]	[illegible]	0	0	0	0	0	0	0	0	0
dos_mqtt_publish	0	1	0	36	8350	0	0	0	0	0	29	0	0	0	0	0	0	0	0
dos_udp	0	1	0	0	0	172215	0	158	0	0	0	20	0	2	0	0	0	1	0
ddos_mqtt_publish	0	0	1	0	0	0	182593	0	0	0	0	0	4	0	0	0	0	0	0
ddos_icmp	0	0	178	0	0	0	0	361879	0	0	0	1	0	12	0	0	0	0	0
ddos_tcp	0	0	20	0	0	0	0	0	98409	0	0	0	1	2	0	0	0	0	0
dos_syn	0	0	0	3	0	0	0	0	0	3128	0	0	0	0	0	0	0	0	0
dos_tcp	0	0	0	0	0	0	0	0	0	0	8505	0	0	0	0	0	0	0	0
port_scan	0	0	0	0	0	43	0	0	0	0	0	98550	0	0	0	0	0	2	0
dos_icmp	0	0	0	0	0	0	17	0	0	0	0	0	82079	0	0	0	0	0	0
ping_sweep	0	0	0	0	0	0	0	24	2716	0	0	0	0	134812	0	0	1	0	0
vul_scan	44	367	0	0	0	0	0	0	0	0	0	0	0	0	1325	4	0	6	1
arp_spoofing	5	241	0	0	0	0	0	0	0	0	0	0	0	0	1	2163	0	1414	10
malformed_mqtt	12	37	0	0	0	0	0	0	0	0	0	0	0	0	0	0	137	0	0
dos_mqtt_connect	63	128	0	0	0	0	0	0	0	0	0	1	0	0	0	424	0	21935	71
os_scan	2	285	0	0	0	0	0	0	0	0	0	0	0	0	2	72	81	141	451

Gambar 4. 9 *Confusion Matrix* RF 10 Fitur data uji

10 fitur terbaik yang digunakan untuk menghasilkan model *machine learning* tersebut dapat dilihat pada gam 4.10



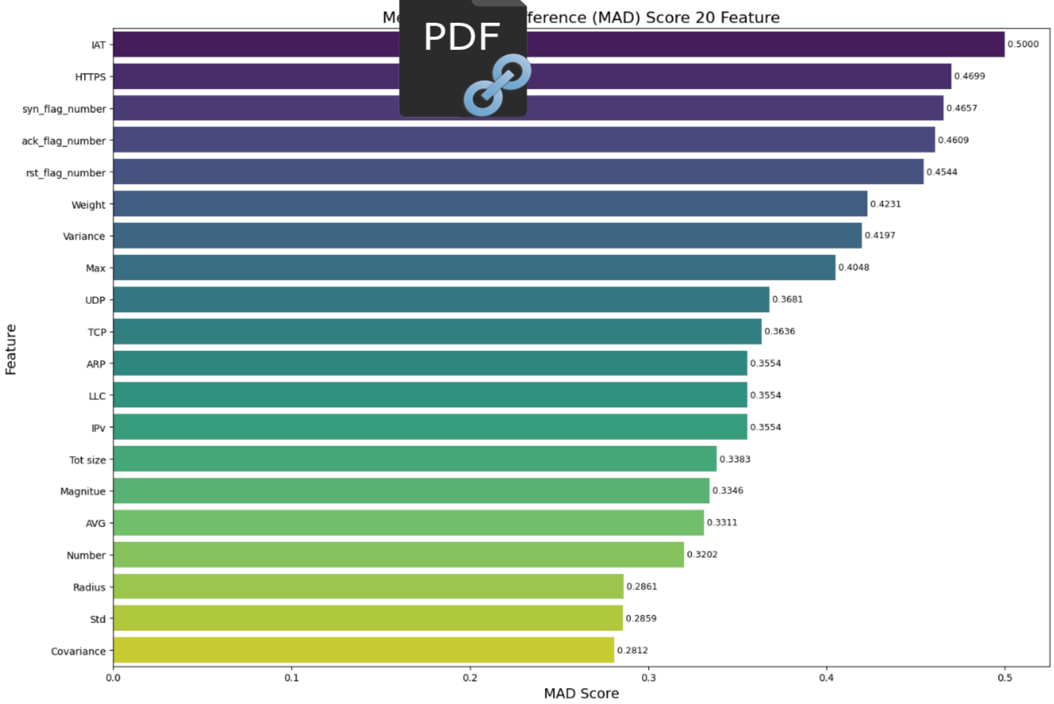
Gambar 4. 10 Nilai bobot 10 fitur menggunakan MAD



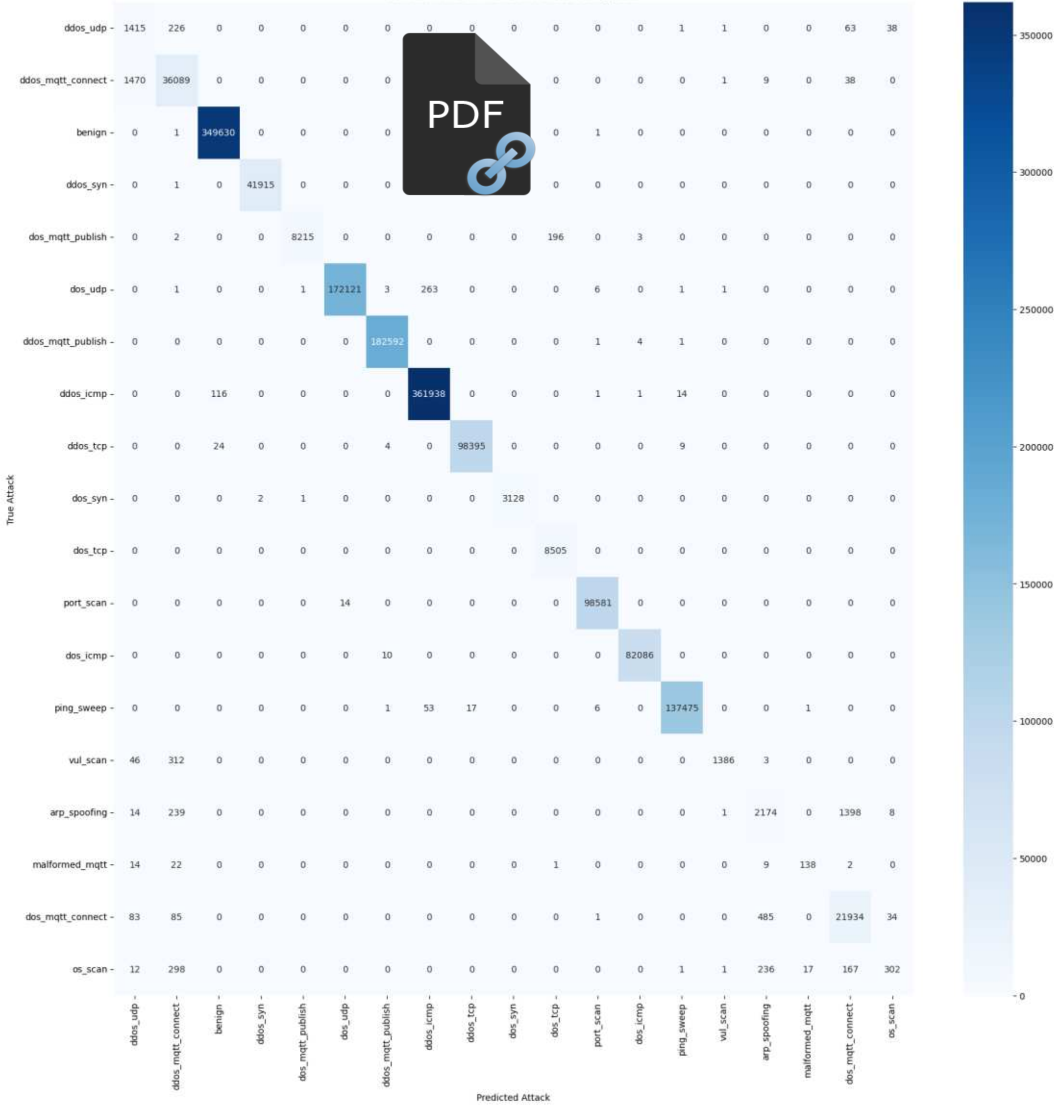
True Attack	ddos_udp	ddos_mqtt_connect	benign	ddos_syn	dos_mqtt_publish	dos_udp	ddos_mqtt_publish	ddos_icmp	ddos_tcp	dos_syn	dos_tcp	port_scan	dos_icmp	ping_sweep	vul_scan	arp_spoofing	malformed_mqtt	dos_mqtt_connect	os_scan
ddos_udp	884	844	1	0	0	0	0	0	14	0	0	0	0	1	0	0	0	0	0
ddos_mqtt_connect	18	37344	0	0	0	0	0	[illegible]	[illegible]	[illegible]	0	0	0	0	0	5	0	3	0
benign	0	2	349686	0	0	0	0	[illegible]	[illegible]	[illegible]	0	0	0	0	0	0	0	0	0
ddos_syn	0	3	0	41901	0	0	0	[illegible]	[illegible]	[illegible]	0	0	0	0	0	0	0	1	0
dos_mqtt_publish	0	3	29	0	5927	0	0	0	2438	0	17	0	2	0	0	0	0	0	0
dos_udp	0	1	54	0	0	172121	1	194	0	0	0	25	0	1	0	0	0	0	0
ddos_mqtt_publish	0	0	146	0	0	0	182445	0	2	0	0	3	2	0	0	0	0	0	0
ddos_icmp	0	0	131455	0	0	0	0	230603	2	0	0	0	0	10	0	0	0	0	0
ddos_tcp	0	0	30	0	0	0	0	0	98401	0	0	0	1	0	0	0	0	0	0
dos_syn	0	0	0	5	1	0	0	0	1	3124	0	0	0	0	0	0	0	0	0
dos_tcp	0	0	9	0	0	0	0	0	2315	0	6181	0	0	0	0	0	0	0	0
port_scan	0	0	7	1	0	37	0	0	5	0	0	98542	0	0	0	0	0	3	0
dos_icmp	0	0	67	0	0	0	14	0	840	0	0	0	81175	0	0	0	0	0	0
ping_sweep	0	0	2	0	0	0	0	23	134144	0	0	0	0	3383	0	0	1	0	0
vul_scan	6	645	10	0	0	0	0	0	0	0	0	0	0	0	1079	2	0	5	0
arp_spoofing	0	292	1	0	0	0	0	0	0	0	0	0	0	0	1	2137	0	1399	4
malformed_mqtt	8	54	0	0	0	0	0	0	1	0	0	0	0	0	0	6	117	0	0
dos_mqtt_connect	3	454	1	0	0	0	0	0	25	0	0	0	0	0	0	639	0	21489	11
os_scan	1	486	0	0	0	0	0	0	1	0	0	0	0	0	0	106	77	142	221

Gambar 4. 11 *Confusion Matrix* RF 20 Fitur data uji

20 fitur terbaik yang digunakan untuk menghasilkan model *machine learning* tersebut dapat dilihat pada gambar 4.12

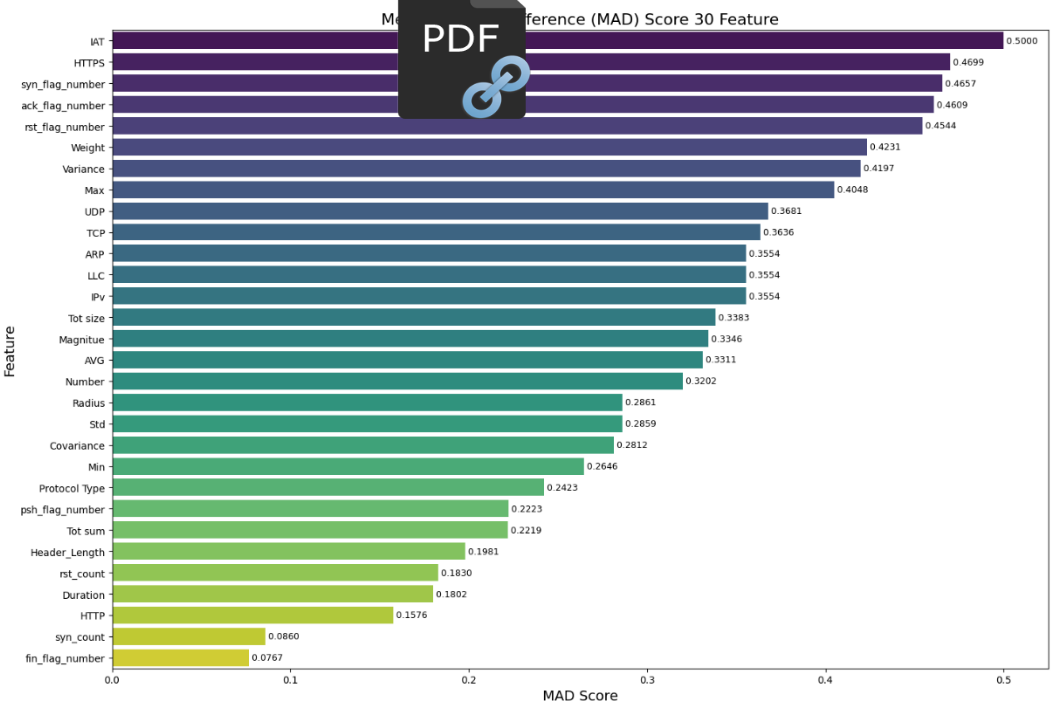


Gambar 4. 12 Nilai bobot 20 fitur menggunakan MAD

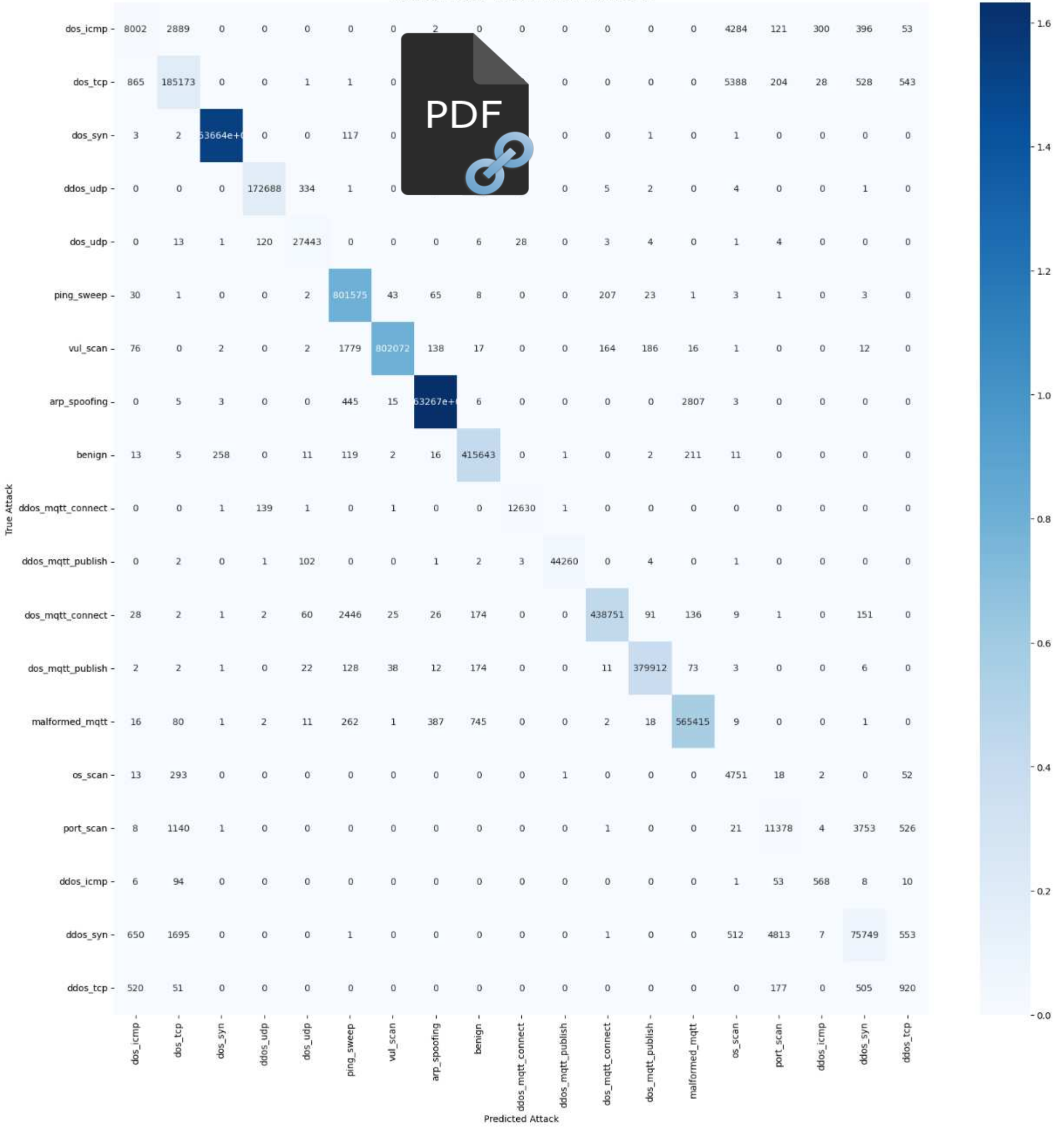


Gambar 4. 13 *Confusion Matrix* RF 30 Fitur data uji

30 fitur terbaik yang digunakan untuk menghasilkan model *machine learning* tersebut dapat dilihat pada gamb 4.14



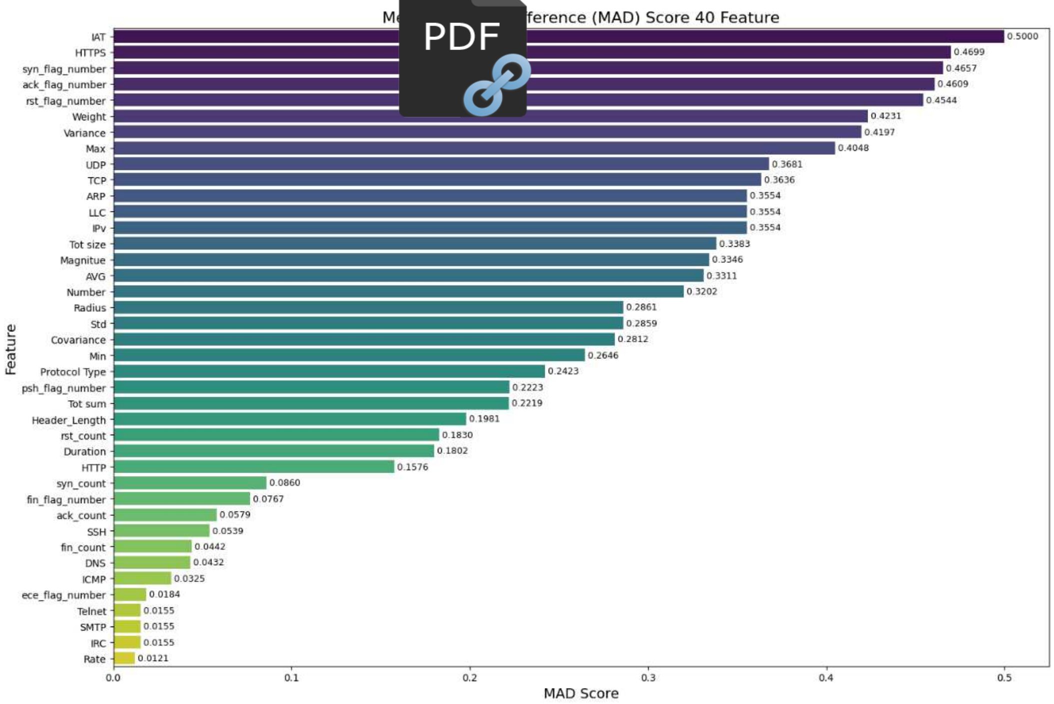
Gambar 4. 14 Nilai bobot 30 fitur menggunakan MAD



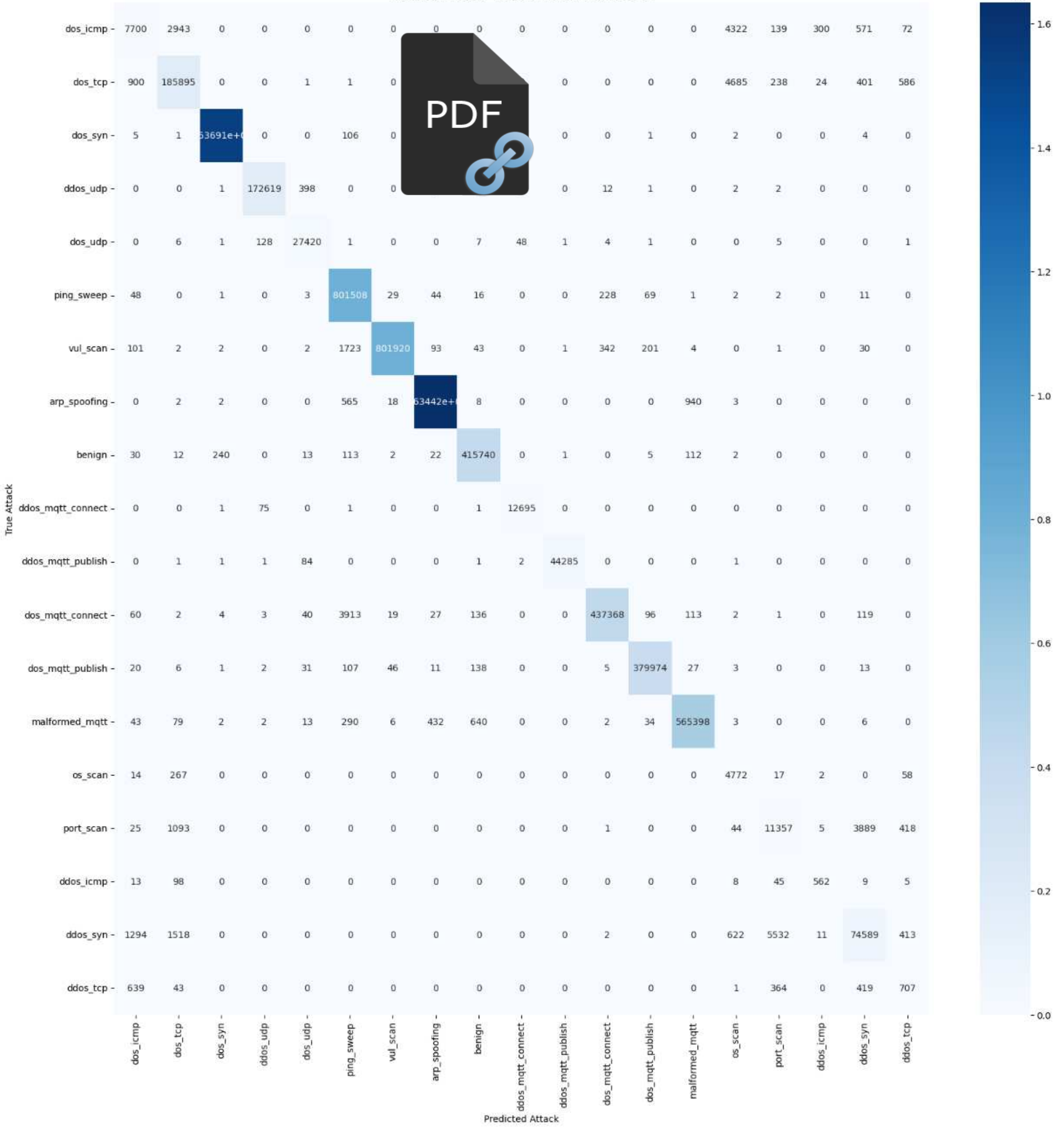
	dos_icmp	dos_tcp	dos_syn	ddos_udp	dos_udp	ping_sweep	vul_scan	arp_spoofing	benign	ddos_mqtt_connect	ddos_mqtt_publish	dos_mqtt_connect	dos_mqtt_publish	malformed_mqtt	os_scan	port_scan	ddos_icmp	ddos_syn	ddos_tcp
dos_icmp	8002	2889	0	0	0	0	0	2	0	0	0	0	0	0	4284	121	300	396	53
dos_tcp	865	185173	0	0	1	1	0	[illegible]	[illegible]	[illegible]	0	0	0	0	5388	204	28	528	543
dos_syn	3	2	63664e+	0	0	117	0	[illegible]	[illegible]	[illegible]	0	0	1	0	1	0	0	0	0
ddos_udp	0	0	0	172688	334	1	0	[illegible]	[illegible]	[illegible]	0	5	2	0	4	0	0	1	0
dos_udp	0	13	1	120	27443	0	0	0	6	28	0	3	4	0	1	4	0	0	0
ping_sweep	30	1	0	0	2	801575	43	65	8	0	0	207	23	1	3	1	0	3	0
vul_scan	76	0	2	0	2	1779	802072	138	17	0	0	164	186	16	1	0	0	12	0
arp_spoofing	0	5	3	0	0	445	15	63267e+	6	0	0	0	0	2807	3	0	0	0	0
benign	13	5	258	0	11	119	2	16	415643	0	1	0	2	211	11	0	0	0	0
ddos_mqtt_connect	0	0	1	139	1	0	1	0	0	12630	1	0	0	0	0	0	0	0	0
ddos_mqtt_publish	0	2	0	1	102	0	0	1	2	3	44260	0	4	0	1	0	0	0	0
dos_mqtt_connect	28	2	1	2	60	2446	25	26	174	0	0	438751	91	136	9	1	0	151	0
dos_mqtt_publish	2	2	1	0	22	128	38	12	174	0	0	11	379912	73	3	0	0	6	0
malformed_mqtt	16	80	1	2	11	262	1	387	745	0	0	2	18	565415	9	0	0	1	0
os_scan	13	293	0	0	0	0	0	0	0	0	1	0	0	0	4751	18	2	0	52
port_scan	8	1140	1	0	0	0	0	0	0	0	0	1	0	0	21	11378	4	3753	526
ddos_icmp	6	94	0	0	0	0	0	0	0	0	0	0	0	0	1	53	568	8	10
ddos_syn	650	1695	0	0	0	1	0	0	0	0	0	1	0	0	512	4813	7	75749	553
ddos_tcp	520	51	0	0	0	0	0	0	0	0	0	0	0	0	0	177	0	505	920

Gambar 4. 15 *Confusion Matrix* RF 40 Fitur data uji

40 fitur terbaik yang digunakan untuk menghasilkan model *machine learning* tersebut dapat dilihat pada gamb[illegible] 4.16

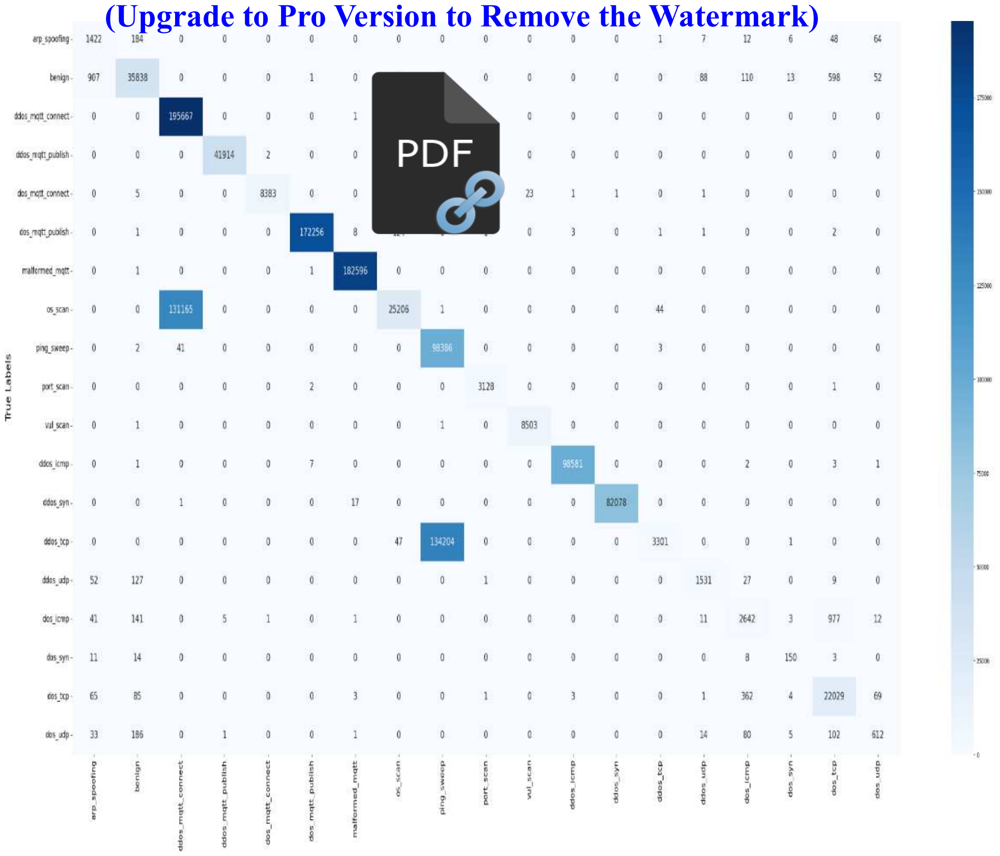


Gambar 4. 16 Nilai bobot 40 fitur menggunakan MAD



	dos_icmp	dos_tcp	dos_syn	ddos_udp	dos_udp	ping_sweep	vul_scan	arp_spoofing	benign	ddos_mqtt_connect	ddos_mqtt_publish	dos_mqtt_connect	dos_mqtt_publish	malformed_mqtt	os_scan	port_scan	ddos_icmp	ddos_syn	ddos_tcp
dos_icmp	7700	2943	0	0	0	0	0	0	0	0	0	0	0	0	4322	139	300	571	72
dos_tcp	900	185895	0	0	1	1	0	[illegible]	[illegible]	[illegible]	0	0	0	0	4685	238	24	401	586
dos_syn	5	1	63691e+	0	0	106	0	[illegible]	[illegible]	[illegible]	0	0	1	0	2	0	0	4	0
ddos_udp	0	0	1	172619	398	0	0	[illegible]	[illegible]	[illegible]	0	12	1	0	2	2	0	0	0
dos_udp	0	6	1	128	27420	1	0	0	7	48	1	4	1	0	0	5	0	0	1
ping_sweep	48	0	1	0	3	801508	29	44	16	0	0	228	69	1	2	2	0	11	0
vul_scan	101	2	2	0	2	1723	801920	93	43	0	1	342	201	4	0	1	0	30	0
arp_spoofing	0	2	2	0	0	565	18	63442e+	8	0	0	0	0	940	3	0	0	0	0
benign	30	12	240	0	13	113	2	22	415740	0	1	0	5	112	2	0	0	0	0
ddos_mqtt_connect	0	0	1	75	0	1	0	0	1	12695	0	0	0	0	0	0	0	0	0
ddos_mqtt_publish	0	1	1	1	84	0	0	0	1	2	44285	0	0	0	1	0	0	0	0
dos_mqtt_connect	60	2	4	3	40	3913	19	27	136	0	0	437368	96	113	2	1	0	119	0
dos_mqtt_publish	20	6	1	2	31	107	46	11	138	0	0	5	379974	27	3	0	0	13	0
malformed_mqtt	43	79	2	2	13	290	6	432	640	0	0	2	34	565398	3	0	0	6	0
os_scan	14	267	0	0	0	0	0	0	0	0	0	0	0	0	4772	17	2	0	58
port_scan	25	1093	0	0	0	0	0	0	0	0	0	1	0	0	44	11357	5	3889	418
ddos_icmp	13	98	0	0	0	0	0	0	0	0	0	0	0	0	8	45	562	9	5
ddos_syn	1294	1518	0	0	0	0	0	0	0	0	0	2	0	0	622	5532	11	74589	413
ddos_tcp	639	43	0	0	0	0	0	0	0	0	0	0	0	0	1	364	0	419	707

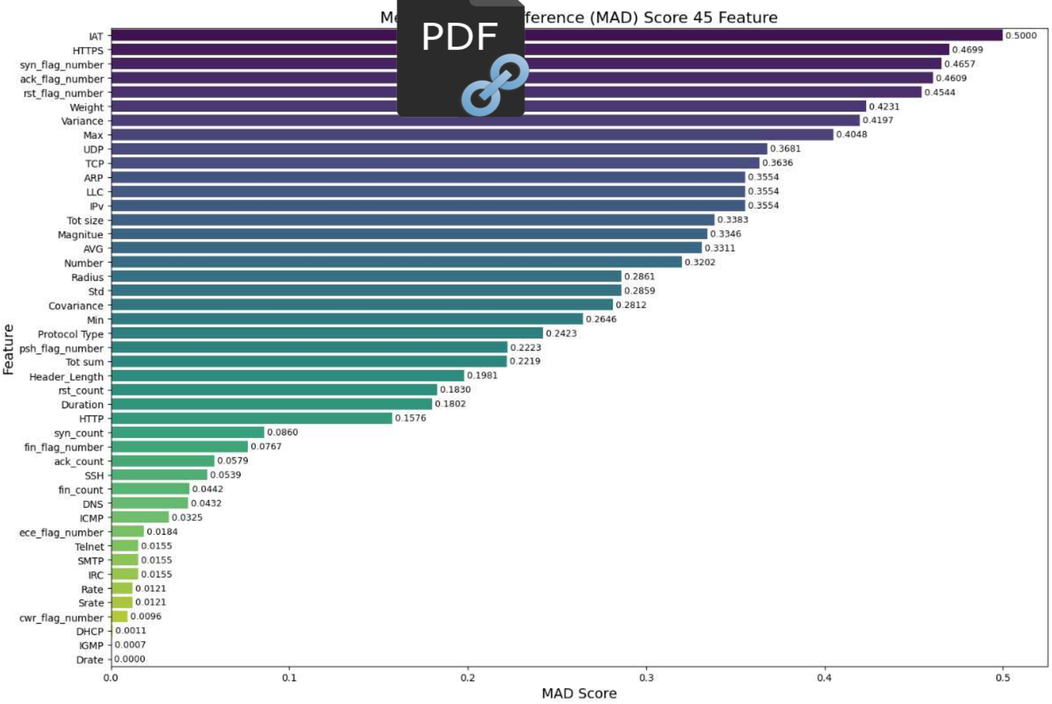
Gambar 4. 17 *Confusion Matrix* RF Tanpa pemilihan Fitur data uji



	arp_spoofing	benign	ddos_mqtt_connect	ddos_mqtt_publish	dos_mqtt_connect	dos_mqtt_publish	malformed_mqtt	os_scan	ping_sweep	port_scan	vul_scan	ddos_icmp	ddos_syn	ddos_tcp	ddos_udp	dos_icmp	dos_syn	dos_tcp	dos_udp
arp_spoofing	1422	184	0	0	0	0	0	0	0	0	0	0	0	1	7	12	6	48	64
benign	907	35838	0	0	0	1	0	[illegible]	[illegible]	0	0	0	0	0	88	110	13	598	52
ddos_mqtt_connect	0	0	195667	0	0	0	1	[illegible]	[illegible]	[illegible]	0	0	0	0	0	0	0	0	0
ddos_mqtt_publish	0	0	0	41914	2	0	0	[illegible]	[illegible]	[illegible]	0	0	0	0	0	0	0	0	0
dos_mqtt_connect	0	5	0	0	8383	0	0	[illegible]	[illegible]	[illegible]	23	1	1	0	1	0	0	0	0
dos_mqtt_publish	0	1	0	0	0	172256	8	[illegible]	[illegible]	[illegible]	0	3	0	1	1	0	0	2	0
malformed_mqtt	0	1	0	0	0	1	182596	0	0	0	0	0	0	0	0	0	0	0	0
os_scan	0	0	131165	0	0	0	0	25206	1	0	0	0	0	44	0	0	0	0	0
ping_sweep	0	2	41	0	0	0	0	0	98386	0	0	0	0	3	0	0	0	0	0
port_scan	0	0	0	0	0	2	0	0	0	3128	0	0	0	0	0	0	0	1	0
vul_scan	0	1	0	0	0	0	0	0	1	0	8503	0	0	0	0	0	0	0	0
ddos_icmp	0	1	0	0	0	7	0	0	0	0	0	98581	0	0	0	2	0	3	1
ddos_syn	0	0	1	0	0	0	17	0	0	0	0	0	82078	0	0	0	0	0	0
ddos_tcp	0	0	0	0	0	0	0	47	134204	0	0	0	0	3301	0	0	1	0	0
ddos_udp	52	127	0	0	0	0	0	0	0	1	0	0	0	0	1531	27	0	9	0
dos_icmp	41	141	0	5	1	0	1	0	0	0	0	0	0	0	11	2642	3	977	12
dos_syn	11	14	0	0	0	0	0	0	0	0	0	0	0	0	0	8	150	3	0
dos_tcp	65	85	0	0	0	0	3	0	0	1	0	3	0	0	1	362	4	22029	69
dos_udp	33	186	0	1	0	0	1	0	0	0	0	0	0	0	14	80	5	102	612

Gambar 4. 18 *Confusion Matrix* GB Tanpa pemilihan Fitur data uji

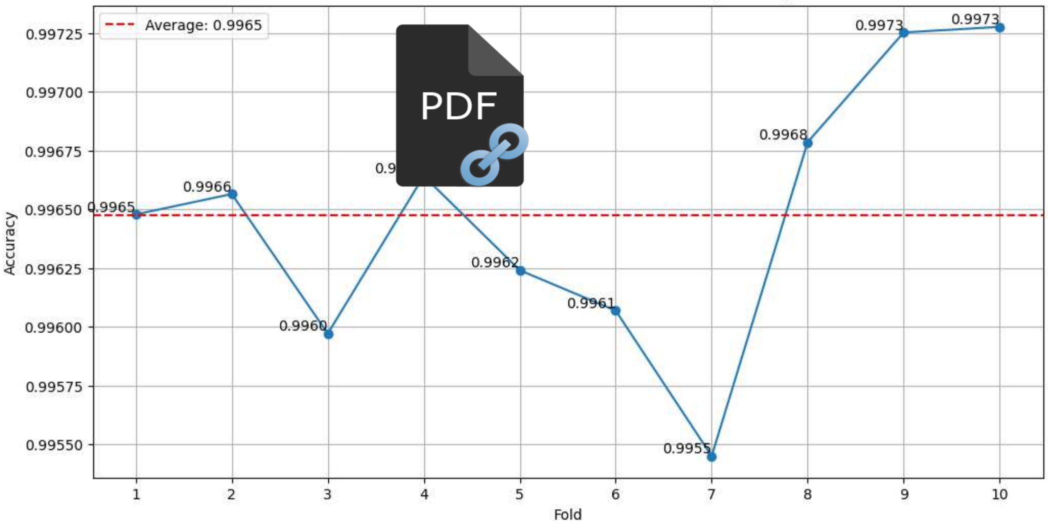
45 fitur terbaik yang digunakan untuk menghasilkan model *machine learning* tersebut dapat dilihat pada gambar 4.19



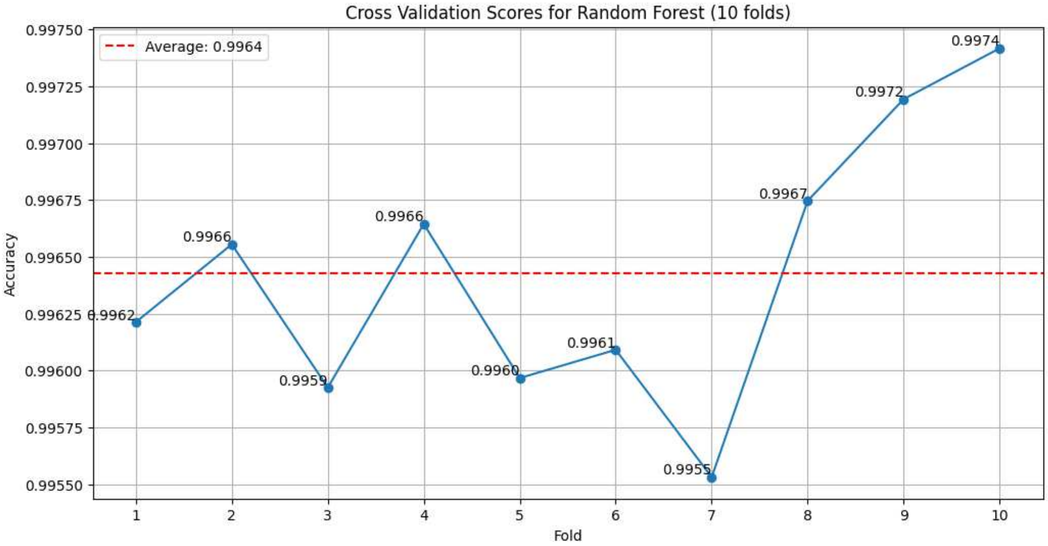
Gambar 4. 19 Nilai bobot semua fitur menggunakan MAD

Hasil evaluasi performa model *machine learning* menunjukkan bahwa algoritma *Random Forest* menghasilkan kinerja yang lebih tinggi dibandingkan dengan algoritma *Gradient Boosting*. Hal ini terlihat dari nilai akurasi *Random Forest* yang mencapai 100% ketika menggunakan tanpa pemilihan fitur. Untuk memastikan validitas model *machine learning* yang dikembangkan, penulis menerapkan teknik *10-fold cross-validation*, yang digunakan untuk memvalidasi hasil model secara menyeluruh dan mengurangi risiko bias dalam evaluasi performa.

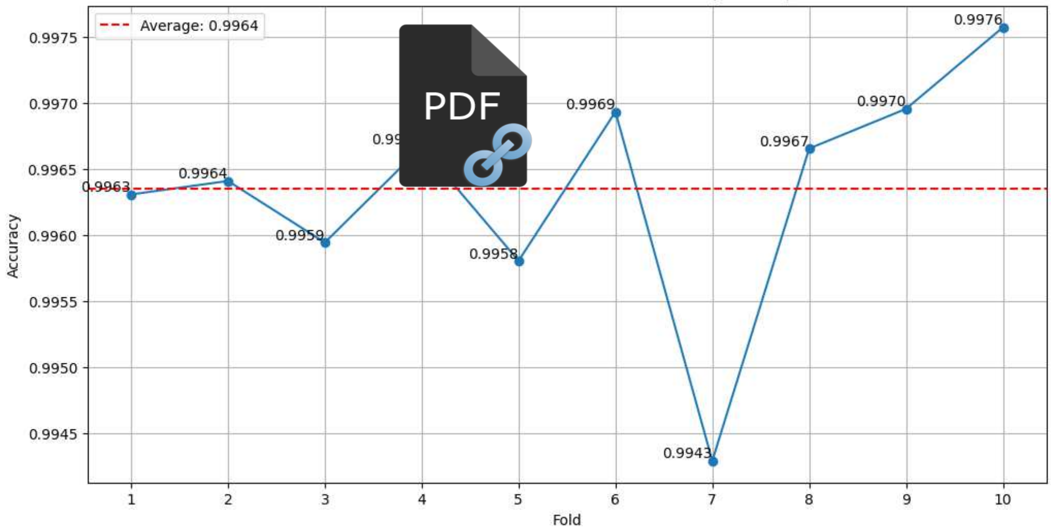
Pada gambar 4.20 sampai gambar 4.24 menunjukkan grafik hasil validasi model *machine learning* untuk algoritma *Random Forest* untuk setiap fitur yang digunakan. Pada gambar 4.25 menunjukkan grafik hasil validasi model *machine learning* untuk algoritma *Gradient Boosting* untuk setiap fitur yang digunakan.



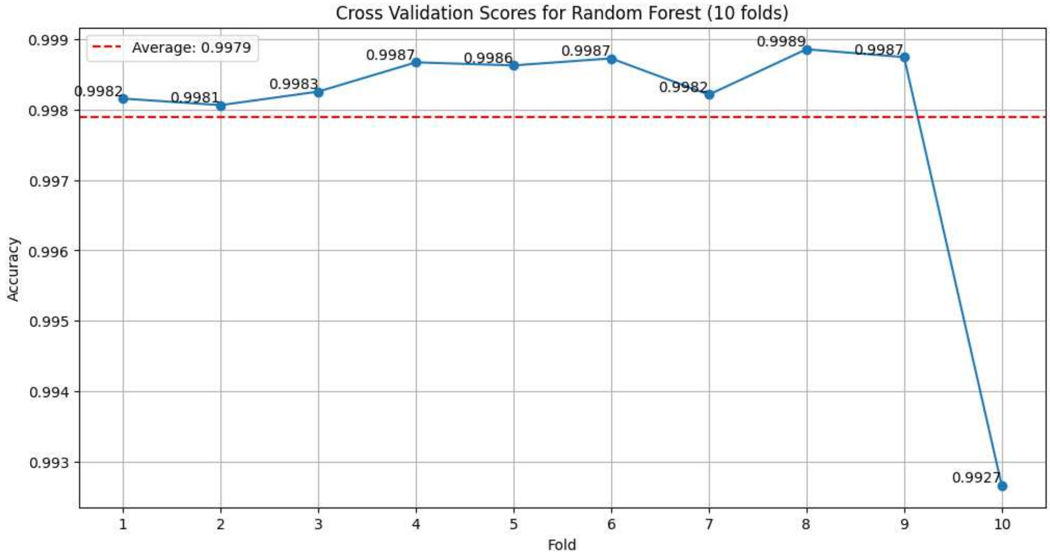
Gambar 4. 20 Hasil pengujian *cross-validation* RF 10 fitur



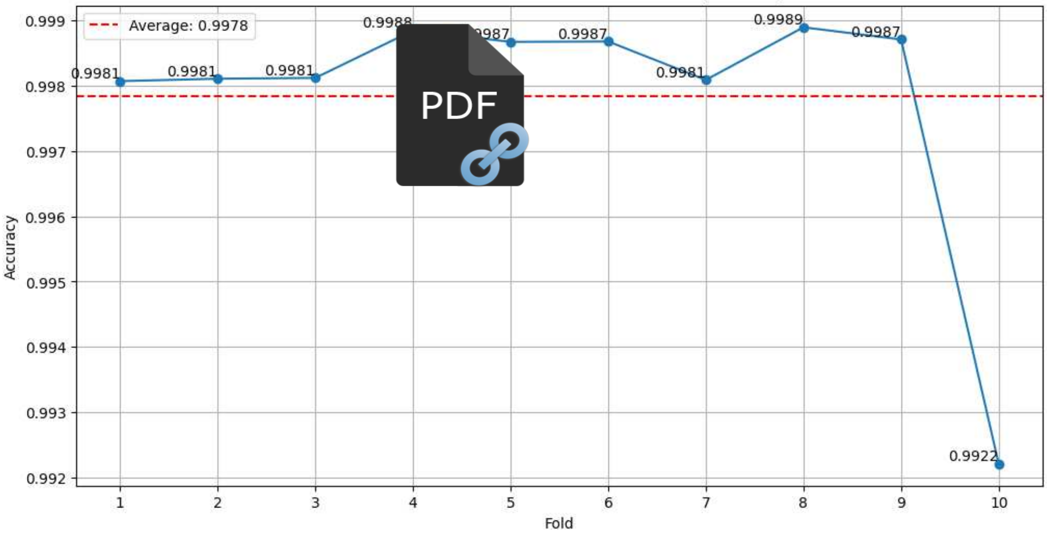
Gambar 4. 21 Hasil pengujian *cross-validation* RF 20 fitur



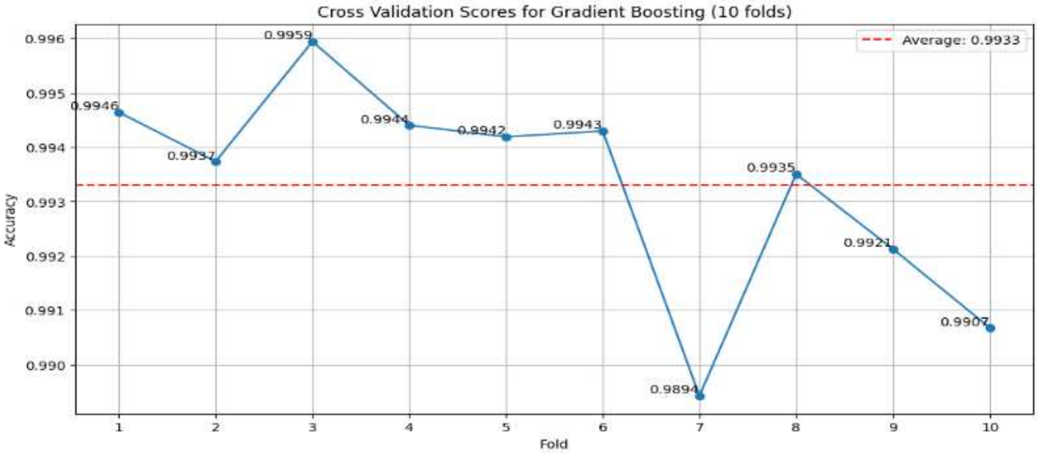
Gambar 4. 22 Hasil pengujian *cross-validation* RF 30 fitur



Gambar 4. 23 Hasil pengujian *cross-validation* RF 40 fitur



Gambar 4. 24 Hasil pengujian *cross-validation* RF Tanpa pemilihan fitur



Gambar 4. 25 Hasil pengujian *cross-validation* GB Tanpa pemilihan fitur

BAB V

KESIM[illegible]AN DAN SARAN

5.1 Kesimpulan

Dari hasil yang di[illegible]ua algoritma menunjukkan kinerja yang sangat baik dengan akurasi yang tinggi serta performa yang memuaskan. *Random Forest* mencatatkan akurasi yang lebih tinggi dibandingkan dengan *Gradient Boosting*. Nilai *precision,* dan *F1-score* juga menunjukkan hasil yang signifikan. Beberapa model algoritma mengalami *overfitting*, sementara yang lainnya tidak, yang dibuktikan melalui hasil *cross-validation*. Hasil *cross-validation* menunjukkan nilai yang hampir sama dengan akurasi yang diperoleh, meskipun terdapat sedikit perbedaan di beberapa model.

Dapat disimpulkan bahwa hasil penelitian ini menunjukkan bahwa penggunaan metode fitur ***Mean Absolute Difference (MAD)*** cukup efektif dalam meningkatkan akurasi model. Hal ini dibuktikan dengan akurasi yang sangat tinggi, mencapai 100%, terutama ketika menggunakan algoritma *Random Forest* dengan semua fitur yang dipilih.

5.2 Saran

Dalam penelitian ini, kendala utama yang dihadapi adalah keterbatasan sumber daya komputasi, di mana pelatihan model menggunakan algoritma *Gradient Boosting* sering terhenti akibat *runtime* Google Colab yang terputus, serta performa laptop yang tidak memadai untuk menangani dataset berukuran besar. Untuk penelitian selanjutnya, metode yang sama dapat diterapkan pada dataset ini dengan menggunakan algoritma lain, seperti *Logistic Regression* dan *Naive Bayes*, untuk mengeksplorasi performa mereka dalam mendeteksi serangan. Selain itu, metode alternatif seperti *correlation analysis* juga dapat digunakan untuk membandingkan hasil seleksi fitur dan efektivitas model yang dihasilkan. Pendekatan ini diharapkan dapat memberikan wawasan lebih luas mengenai optimalisasi model dan metode dalam mendeteksi ancaman siber secara lebih efisien.

DAFTAR PUSTAKA

[1] Aljumaie, G. S., Alzeer, [illegible]lghamdi, R. K., Alsuwat, H., & Alsuwat, E. (2021). Modern s[illegible] internet of medical things (IOMT) security. *International Journal of Computer Science & Network Security*, *21*(8), 254-266.

[2] Ali, S. E., Tariq, N., Khan, F. A., Ashraf, M., Abdul, W., & Saleem, K. (2023). BFT-IOMT: A blockchain-based trust mechanism to mitigate SyBiL attack using fuzzy logic in the internet of medical things. *Sensors*, *23*(9), 4265.

[3] Ghubaish, A., Salman, T., Zolanvari, M., Unal, D., Al-Ali, A., & Jain, R. (2020). Recent advances in the internet-of-medical-things (IoMT) systems security. *IEEE Internet of Things Journal*, *8*(11), 8707-8718.

[4] Ahmed, S. F., Alam, M. S. B., Afrin, S., Rafa, S. J., Rafa, N., & Gandomi, A. H. (2024). Insights into Internet of Medical Things (IoMT): Data fusion, security issues and potential solutions. *Information Fusion*, *102*, 102060.

[5] Sun, Y., Lo, F. P. W., & Lo, B. (2019). Security and privacy for the internet of medical things enabled healthcare systems: A survey. *IEEE Access*, *7*, 183339-183355.

[6] Dadkhah, S., Neto, E. C. P., Ferreira, R., Molokwu, R. C., Sadeghi, S., & Ghorbani, A. (2024). Ciciomt2024: Attack vectors in healthcare devices-a multi-protocol dataset for assessing iomt device security.

[7] Adnan, A., Muhammed, A., Abd Ghani, A. A., Abdullah, A., & Hakim, F. (2021). An intrusion detection system for the internet of things based on machine learning: Review and challenges. *Symmetry*, *13*(6), 1011.

[8] Guyon, I., & Elisseeff, A. (2003). An introduction to variable and feature selection. *Journal of machine learning research*, *3*(Mar), 1157-1182.

[9] Santo, W. B., Syukur, A., & Purwanto, P. (2024). Pemilihan Fitur Menggunakan Algoritma Chi-Square Dan Particle Swarm Optimization (PSO) Untuk Meningkatkan Kinerja Deep Neural Network Pada Deteksi Penyakit Diabetes. *JURNAL MEDIA INFORMATIKA BUDIDARMA*, *8*(1), 488-496.

[10] Pinsky, E., & Klawansky, S. (2023). MAD (about median) vs. quantile-based alternatives for classical standard deviation, skewness, and kurtosis. *Frontiers in Applied Mathematics and Statistics*, *9*, 1206537.

[11] Stiawan, D., Arifin, M. A. S., Idris, M. Y., & Budiarto, R. (2020, October). IoT botnet malware classification Using Weka Tool and scikit-learn machine learning. In 2[illegible] *International Conference on Electrical Engineering, Computer [illegible] and Informatics (EECSI)* (pp. 15-20). IEEE.

[12] Upadhyay, D., Manero, J., Zaman, M., & Sampalli, S. (2020). Gradient boosting feature selection with machine learning classifiers for intrusion detection on power grids. *IEEE Transactions on Network and Service Management*, *18*(1), 1104-1116.

[13] Saroji, Ahmad & Harmini, Triana & Taqiyuddin, Muhammad. (2021). Internet Evolution: A Historical View (SEJARAH EVOLUSI GENERASI INTERNET). Walasuji Jurnal Sejarah dan Budaya. 2. 65-75. 10.30598/Lanivol2iss2page65-75.

[14] Erwin, Erwin & Datya, Aulia & Nurohim, & M.Kom, Sepriano & Waryono, Waryono & Adhicandra, Iwan & Budihartono, Eko & Purnawati, Ni. (2023). PENGANTAR & PENERAPAN INTERNET OF THINGS: Konsep Dasar & Penerapan IoT Di Berbagai Sektor.

[15] Tariq, U., Ullah, I., Yousuf Uddin, M., & Kwon, S. J. (2022). An effective self-configurable ransomware prevention technique for IOMT. *Sensors*, *22*(21), 8516.

[16] Mukhopadhyay, M., Banerjee, S., & Mukhopadhyay, C. D. (2024). Internet of Medical Things and the Evolution of Healthcare 4.0: Exploring Recent Trends. *Journal of Electronics, Electromedical Engineering, and Medical Informatics*, *6*(2), 182-195.

[17] Rasheed, A. F., Zarkoosh, M., & Al-Azzawi, S. S. (2023, August). The impact of feature selection on malware classification using chi-square and machine learning. In *2023 9th International Conference on Computer and Communication Engineering (ICCCE)* (pp. 211-216). IEEE.

[18] Balaraman, S. (2020). Comparison of classification models for breast cancer identification using Google Colab.

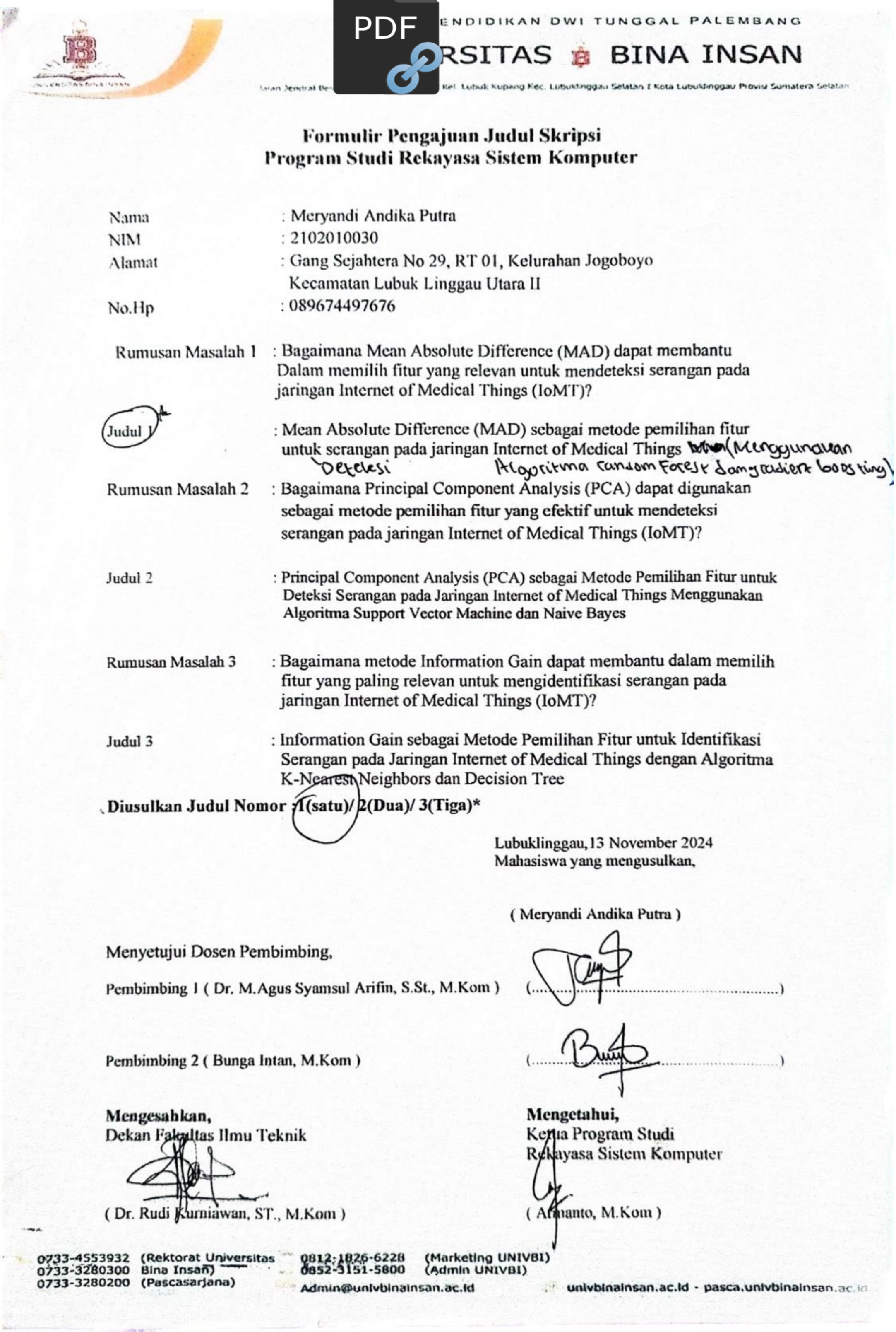
[19] Zuhal, N. K. (2022, February). Study Comparison K-Means Clustering Dengan Algoritma Hierarchical Clustering: AHC, K-Means Clustering, Study Comparison. In *Seminar Nasional Teknologi & Sains* (Vol. 1, No. 1, pp. 200-205).

[20] Jalil, A., Homaidi, A., & Fatah, Z. (2024). Implementasi Algoritma Support Vector Machine Untuk Klasifikasi Status Stunting Pada Balita. *G-Tech: Jurnal Teknologi Terapan*, *8*(3), 2070-2079.

[21] Rustamana, A., Wahyuningsih, P., Azka, M. F., & Wahyu, P. (2024). Penelitian metode kuantitatif. *Sindoro: Cendikia Pendidikan*, *5*(6), 81-90.

[22] Riyadani, M. E., & Sub[illegible] (2022). Sistem keamanan untuk otorisasi pada smart home m[illegible]an pengenalan wajah dengan library openCV. *Jurnal SISK[illegible] (Sistem Komputer dan Kecerdasan Buatan)*, *5*(2), 69-77.

DAFTAR LAMPIRAN



ENDIDIKAN DWI TUNGGAL PALEMBANG
RSITAS BINA INSAN
alan Jendral Be Kel. Lubuk Kupang Kec. Lubuklinggau Selatan I Kota Lubuklinggau Provisi Sumatera Selatan

Formulir Pengajuan Judul Skripsi
Program Studi Rekayasa Sistem Komputer

Nama : Meryandi Andika Putra
NIM : 2102010030
Alamat : Gang Sejahtera No 29, RT 01, Kelurahan Jogoboyo
Kecamatan Lubuk Linggau Utara II
No.Hp : 089674497676

Rumusan Masalah 1 : Bagaimana Mean Absolute Difference (MAD) dapat membantu Dalam memilih fitur yang relevan untuk mendeteksi serangan pada jaringan Internet of Medical Things (IoMT)?

Judul 1 : Mean Absolute Difference (MAD) sebagai metode pemilihan fitur untuk Deteksi serangan pada jaringan Internet of Medical Things (Menggunakan Algoritma random Forest dan gradient boosting)

Rumusan Masalah 2 : Bagaimana Principal Component Analysis (PCA) dapat digunakan sebagai metode pemilihan fitur yang efektif untuk mendeteksi serangan pada jaringan Internet of Medical Things (IoMT)?

Judul 2 : Principal Component Analysis (PCA) sebagai Metode Pemilihan Fitur untuk Deteksi Serangan pada Jaringan Internet of Medical Things Menggunakan Algoritma Support Vector Machine dan Naive Bayes

Rumusan Masalah 3 : Bagaimana metode Information Gain dapat membantu dalam memilih fitur yang paling relevan untuk mengidentifikasi serangan pada jaringan Internet of Medical Things (IoMT)?

Judul 3 : Information Gain sebagai Metode Pemilihan Fitur untuk Identifikasi Serangan pada Jaringan Internet of Medical Things dengan Algoritma K-Nearest Neighbors dan Decision Tree

Diusulkan Judul Nomor [✓ 1(satu)]/ 2(Dua)/ 3(Tiga)*

Lubuklinggau, 13 November 2024
Mahasiswa yang mengusulkan,

(Meryandi Andika Putra)

Menyetujui Dosen Pembimbing,

Pembimbing 1 (Dr. M.Agus Syamsul Arifin, S.St., M.Kom) (..............................)

Pembimbing 2 (Bunga Intan, M.Kom) (..............................)

Mengesahkan,
Dekan Fakultas Ilmu Teknik

(Dr. Rudi Kurniawan, ST., M.Kom)

Mengetahui,
Ketua Program Studi
Rekayasa Sistem Komputer

(Armanto, M.Kom)

0733-4553932 (Rektorat Universitas Bina Insan)
0733-3280300
0733-3280200 (Pascasarjana)
0812-1826-6228 (Marketing UNIVBI)
0852-3151-5800 (Admin UNIVBI)
Admin@univbinainsan.ac.id
univbinainsan.ac.id - pasca.univbinainsan.ac.id