KLASIFIKASI SERANGAN DDOS PADA JARINGAN IOMT MENGGUNAKAN *SUPPORT VECTOR MACHINE* DENGAN *KER POLYNOMIAL*

SKRIPSI

Diajukan Sebagai Syarat Untuk Menyelesaikan Pendidikan
Program Sarjana (S-1)
Pada Program Studi Rekayasa Sistem Komputer

Oleh :
MUHAMMAD AGUNG PRAYOGI
NIM :2102010039

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

HALAMAN PENGESAHAN SKRIPSI

KLASIFIKASI SERANGAN DOS PADA JARINGAN IOMT MENGGUNAKAN *SUPPORT VECTOR MACHINE* DENGAN *KERNEL POLYNOMIAL*

Oleh :
MUHAMMAD AGUNG PRAYOGI
NIM : 2102010039

Lubuklinggau, 25 Januari 2025

Pembimbing I	Pembimbing II
(Harma Oktafia Lingga Wijaya, M.Kom)	(Deni Nurdiansyah, M.Kom)

Mengetahui,
Dekan Fakultas Ilmu Teknik
Universitas Bina Insan

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

HALAMAN PERSETUJUAN TIM PENGUJI SKRIPSI

Pada hari sabtu tanggal 25 bulan Januari tahun 2025 telah dilaksanakan sidang Skripsi oleh Program Studi Rekayasa Sistem Komputer Universitas Bina Insan.

Nama	: Muhammad Agung Prayogi
NIM	: 2102.01.0039
Judul Skripsi	: Klasifiskasi serangan DDoS pada jaringan IoMT Menggunakan *support vector machine* dengan *kernel polynomial*

Komisi Penguji

1. Ketua	: Harma Oktafia Lingga Wijaya, M.Kom	( )
2. Sekretaris	: Deni Nurdiansyah, M.Kom	( )
3. Anggota	: Dr. M. Agus Syamsul Arifin, S.St., M.Kom	( )

Mengetahui,
Kepala Program Studi Rekayasa Sistem Komputer
Universitas Bina Insan

(Armanto, M.Kom)

HALAMAN MOTTO DAN PERSEMBAHAN

MOTTO

- SAYA TIDAK TAU KUNCI [illegible] APA, TAPI SAYA TAU KUNCI GAGAL, YAITU MENYENANGKAN SEMUA ORANG
- TERKADANG SAYA MERASA TIDAK INGIN BEKERJA , TAPI KEMUDIAN SAYA INGAT SAYA TERLAHIR TAMPAN, BUKAN KAYA
- FORTIS FORTUNA ADIUVAT (KEBERUNTUNGAN BERPIHAK PADA YANG BERANI)

PERSEMBAHAN KEPADA :

- *ALLAH SWT YANG TELAH MEMBERIKAN RAHMAT DAN HIDAYAHNYA.*
- *ORANG TUA YANG SELALU SUPPORT DAN MENDOAKANKU.*
- *TERIMA KASIH KEPADA BUNGA LARASATI YANG SUDAH MENEMANI HINGGA SAAT INI*
- *TERIMAKASIH CHAT GPT TELAH MEMBANTU SAYA MENGERJAKAN SEMUA TUGAS SAYA*

HALAMAN PERNYATAAN

Saya yang bertanda tanggan dibawah ini :

Nama : Muhammad Agung Prayogi

Nim : 2102010039

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, 25 Januari 2025

Muhammad Agung Prayogi

ABSTRACT

The Internet of Medical Things (IoMT) is a significant development in the healthcare sector, enabling real-time patient monitoring and enhancing diagnostic efficiency. However, IoMT networks are vulnerable to cyberattacks, especially Distributed Denial of Service (DDoS) attacks, which can compromise the security of sensitive medical data. This study aims to develop a classification model using the Support Vector Machine (SVM) algorithm with a polynomial kernel to detect DDoS attacks on IoMT networks. Utilizing the CICIoMT 2024 dataset, the research measures the model's performance using metrics such as accuracy, precision, recall, and F1-score. The results indicate that the SVM with a polynomial kernel demonstrates high accuracy (83% on training data and 75% on testing data) for most classes, including benign and certain DDoS attack types. Despite its strengths, the model shows limitations in detecting specific attack types, such as DDoS TCP. Cross-validation reveals that the model is stable but has slight overfitting. This research contributes to advancing IoMT security and provides insights for developing more robust intrusion detection systems.

Kata Kunci: *Internet of Medical Things, cybersecurity, DDoS attacks, intrusion detection, Support Vector Machine, polynomial kernel, CICIoMT 2024, machine learning, cross-validation, classification performance.*

ABSTRAK

Internet of Medical Th *T)* merupakan perkembangan signifikan dalam sektor kesehatan yang m nkan pemantauan pasien secara real-time dan meningkatkan efisiensi diagnosis. Namun, jaringan IoMT rentan terhadap serangan siber, khususnya serangan *Distributed Denial of Service (DDoS)* yang dapat membahayakan keamanan data medis yang sensitif. Penelitian ini bertujuan untuk mengembangkan model klasifikasi menggunakan algoritma *Support Vector Machine (SVM)* dengan *kernel polynomial* untuk mendeteksi serangan DDoS pada jaringan IoMT. Dengan memanfaatkan dataset CICIoMT 2024, penelitian ini mengukur performa model menggunakan metrik seperti akurasi, presisi, recall, dan F1-score. Hasil penelitian menunjukkan bahwa SVM dengan *kernel polynomial* memiliki akurasi tinggi (83% pada data latih dan 75% pada data uji) untuk sebagian besar kelas, termasuk benign dan beberapa jenis serangan DDoS tertentu. Meskipun demikian, model ini memiliki keterbatasan dalam mendeteksi jenis serangan tertentu, seperti DDoS TCP. Validasi silang menunjukkan bahwa model cukup stabil namun sedikit mengalami overfitting. Penelitian ini berkontribusi pada peningkatan keamanan IoMT dan memberikan wawasan untuk pengembangan sistem deteksi intrusi yang lebih andal.

Kata Kunci: *Internet of Medical Things*, keamanan siber, serangan DDoS, deteksi intrusi, *Support Vector Machine, kernel polinomial*, CICIoMT 2024, pembelajaran mesin, validasi silang, kinerja klasifikasi.

KATA PENGANTAR

Alhamdulillah puji dan penulis ucapkan kepada Allah SWT atas segala rahmat dan karunia-Nya memberikan kekuatan dan kesempatan, sehingga penulis dapat menyelesaikan Skripsi ini dengan maksimal dan tepat waktu, untuk diajukan sebagai syarat menyelesaikan Pendidikan Strata Satu (S1) pada Program Studi Rekayasa Sistem Komputer, Fakultas Ilmu Teknik Universitas Bina Insan Lubuklinggau. Kemudian sholawat beserta salam semoga tetap tercurahkan kepada baginda Nabi Muhammad SAW, keluarga, sahabat, serta umatnya hingga akhir zaman.

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

Untuk selanjutnya penulis mengucapkan banyak terima kasih kepada pihak-pihak yang telah membantu dalam menyelesaikan Skripsi ini, yaitu:

1. Bapak Dr. H Sardiyo, MM 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, ST., M.Kom Selaku Dekan Fakultas Ilmu Teknik Universitas Bina Insan Lubuklinggau.

5. Bapak Armanto, M.Kom selaku Ketua Prodi Rekayasa Sistem Komputer Universitas Bina Insan Lubuklinggau
6. Ibu Harma Oktafia Lingga, M.Kom selaku pembimbing I yang telah memberikan ilmu, motivasi, perhatian serta bimbingan dalam penyelesaian Proposal Skripsi ini.
7. Bapak Deni Nurdiansyah, M.Kom selaku pembimbing II yang telah memberikan ilmu, motivasi, perhatian serta bimbingan dalam penyelesaian Proposal Skripsi ini.
8. Seluruh Staf Dosen dan Karyawan Universitas Bina Insan yang telah banyak memberikan ilmu pengetahuan dan bimbingan kepada penulis.
9. Orang tua 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 bagi tempat penelitian sertasebagai referensi untuk penelitian selanjutnya.

Lubuklinggau, 25 Januari 2025

Muhammad Agung Prayogi
(2102010039)

DAFTAR RIWAYAT HIDUP

Biodata :

Nama	: Muhammad Agung Prayogi
Tempat/Tanggal Lahir	: LubukLinggau 05 Juli 2003
Jenis Kelamin	: Laki-Laki
Status	: Mahasiswa
Agama	: Islam
Alamat	: Kali Serayu Kecamatan Lubuklinggau Utara II, Kota Lubuklinggau.

Pendidikan :

- SD NEGERI 50 Lubuklinggau
- Madrasah Tsanawiyah Negeri 1 Lubuklingga
- SMA NEGERI 3 Lubuklinggau

TAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

DAFTAR LAMPIRAN

BAB 1
PENDAHULUAN

1.1 Latar Belakang

Internet of Things (IoT) telah memberikan manfaat besar dalam berbagai aspek kehidupan dengan menghubungkan sejumlah besar perangkat pintar. Teknologi ini memungkinkan perangkat-perangkat yang sebelumnya berdiri sendiri untuk saling terhubung melalui internet, menciptakan ekosistem yang terintegrasi. Dengan kemampuan ini, IoT telah membuka peluang baru di berbagai bidang, mulai dari otomatisasi rumah tangga hingga revolusi industri. Selain itu, IoT memungkinkan peningkatan efisiensi, penghematan biaya, dan kemudahan akses informasi secara real-time. Penerapan IoT sangat luas, mencakup sektor-sektor strategis seperti kesehatan [1], pertanian [2] dan industri [3] Bahkan, IoT telah diadopsi dalam kehidupan sehari-hari, seperti pada sistem keamanan rumah yang mempermudah monitoring kondisi dan keamanan lingkungan tempat tinggal [4].

IoT telah berkontribusi signifikan dalam bidang kesehatan melalui pengembangan *Internet of Medical Things (IoMT)*. IoMT memungkinkan interkoneksi perangkat medis untuk pemantauan kondisi pasien secara *real-time*, sehingga mempercepat proses diagnostik [5]. Perkembangan teknologi medis seperti IoMT tidak hanya meningkatkan efisiensi pelayanan kesehatan, tetapi juga meningkatkan keamanan pasien, terutama bagi mereka yang menderita penyakit menular berbahaya [6]. IoT yang diterapkan pada sistem medis disebut *Internet of Medical Things (IoMT)* [7]. IoMT, seperti jaringan IoT pada umumnya, memiliki kerentanan terhadap serangan siber. Risiko ini berasal dari perangkat dalam

jaringan dan protokol komunikasi yang digunakan, seperti MQTT. Protokol MQTT yang lebih memprioritaskan k daripada keamanan menjadi celah bagi ancaman seperti kebocoran data

Salah satu cara untuk mengatasi permasalahan tersebut adalah membuat sebuah model cerdas berbasisi *machine learning* untuk melakukan deteksi serangan pada jaringan IoMT. Model ini akan mendeteksi (mengklasifikasi) serangan dalam jaringan IoMT dengan lebih presisi karena menggunakan data latih yang digunakan diambil dari lalulintas IoMT. Dalam penelitian ini akan menggunakan dataset CICIoMT 2024 dan algoritma *Support Vector Machine*.

Berdasarkan latar belakang tersebut penulis akan mengangkat tema keamanan IoMT menggunakan *machine learning* dengan dataset CICIoMT 2024 [7] dengan judul "**KLASIFIKASI SERANGAN DDOS PADA JARINGAN IOMT MENGGUNAKAN *SUPPORT VECTOR MACHINE* DENGAN *KERNEL POLYNOMIAL***" dimana model yang dibuat akan menggunakan algoritma SVM dengan *kernel polynomial*. Penelitian ini bertujuan untuk mengembangkan model klasifikasi yang mampu mendeteksi serangan *Distributed Denial of Service (DDoS)* secara efektif dalam jaringan IoMT.

1.2 Identifikasi Masalah

Berdasarkan latar belakang yang sudah diuraikan tersebut maka di identifikasi masalah yang akan penulis angkat pada penelitian ini adalah serangan DDoS menjadi ancaman pada sistem IoMT dalam keamanan data pada sistem medis

sehigga data – data sensitif dalam sistem medis menjadi rentan terhadap kebocoran data.

1.3 Rumusan Masalah

Berdasarkan identifikasi diatas maka dapat dirumuskan permasalahan yang ada yaitu, bagaimana algoritma *Support Vector Mahine* dapat diterapkan dalam deteksi serangan siber di lingkungan IoMT untuk mendeteksi serangan DDoS dengan menggunakan dataset CICIoMT 2024 ?

1.4 Batasan Masalah

Agar pembahasan dari perancangan tidak terlalu meluas maka penulis perlu membuat batasan-batasan masalah yang meliputi:

a. Penelitian ini menggunakan dataset CICIoMT 2024 dengan format *Comma Separated Values (CSV).*
b. Penelitian ini menggunakan Algoritma *Support Vector Machine* dengan kernel Polynomial untuk membuat model deteksi serangan DDoS pada dataset IoMT 2024.
c. Penelitian ini tidak disimulasikan dalam jaringan nyata maupun jaringan virtual tapi hanya dengan memodelkan dengan data latih CICIoMT 2024.
d. Penelitian ini tidak membahas pencegahan serangan siber pada jaringan IoMT.
e. Penelitian ini tidak membahas proses ekstraksi data.
f. Penelitian ini hanya diujikan pada data latih yang sudah disediakan pada dataset CICIoMT 2024.

1.5 Tujuan dan Manfaat Penelitian

1.5.1 Tujuan Penelitian

a. Tujuan Umum

Dapat memberi kontribusi dalam metode deteksi serangan dengan menggunakan algoritma *Support Vector Machine*.

b. Tujuan Khusus

Untuk menyelesaikan salah satu syarat dalam penyelesaian tugas akhir di Program Studi Rekayasa Sistem Komputerdi Universitas Bina Insan.

1.5.2 Manfaat Penelitian

Manfaat penelitian ini adalah sebagai berikut:

a. Manfaat bagi Perkembangan IPTEK

Dengan adanya informasi dari hasil penelitian ini maka dapat menambah bahan referensi ilmu pengetahuan dan mempunyai perbandingan bagi peneliti lain yang akan mengkaji penelitian dibidang yang sama.

b. Manfaat bagi Tempat Penelitian

Dengan adanya penelitian ini diharapkan dapat menambah pengetahuan untuk menerapkan algoritma *Support Vector Machine* dalam mendeteksi serangan siber pada jaringan IoMT.

c. Manfaat bagi Peneliti

Dapat menambah pengetahuan bagi peneliti dan manerapkan atau mempraktekan secara langsung teori-teori dan ilmu pengetahuan yang telah dipelajari di Universitas Bina Insan (UNIV BI) Lubuklinggau.

d. Manfaat bagi Lembaga

Menambah bahan referensi atau bahan bacaan tentang ilmu komputer Khususnya mengenai *Security* pada Universitas Bina Insan Lubuklinggau.

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 literatur dan penelitian terdahulu yang relevan, serta kerangka berpikir yang menjadi 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
KAJIAN PUSTAKA

2.1 Literatur

2.1.1 *Internet of Things (I*

Internet of things m mampuan untuk menghubungkan obyek pintar dan memungkinkan perangkat tersebut untuk berinteraksi dengan lingkungan dan peralatan komputasi cerdas lainnya melalui jaringan internet [9]. Semakin bertambahnya perangjat IoT yang terhubung akan menarik penyerang untuk melakukan sabotase dari perangkat – perangkat IoT tersebut khususnya menggunakan malware [10].

2.1.2 Dataset CICIoMT 2024

Dataset CICIoMT 2024 (*Canadian Institute for Cybersecurity Internet of Medical Things*) adalah kumpulan data trafik jaringan yang disediakan oleh *Canadian Institute for Cybersecurity (CIC).* Dataset ini dirancang khusus untuk mendukung penelitian dalam bidang *Internet of Medical Things (IoMT)* dan keamanan siber [7]. CICIoMT 2024 mengandung data lalu lintas jaringan dari perangkat IoMT yang terhubung ke jaringan, termasuk beberapa jenis serangan yang ada di dalamnya.

Dataset ini memiliki beberapa tujuan, termasuk membantu para peneliti dan profesional keamanan untuk menganalisis, menguji, dan mengembangkan metode deteksi serta perlindungan terhadap ancaman siber lainnya dalam konteks lingkungan IoMT.

2.1.3 Klasifikasi

Kamus Besar Baha esia (KBBI) menjelaskan pengertian klasifikasi adalah penyu sistem dalam kelompok atau golongan menurut kaidah atau standar yang ditetapkan [11]. Klasifikasi adalah pengelompokkan sesuatu dengan proses membedakan dan mendistribusikan jenis "hal" ke dalam kelompok yang berbeda. Hasil dari klasifikasi bisa berupa kumpulan kelas. Misalnya, pengelompokan semua pakaian berdasarkan warna dapat memudahkan untuk memilih pakaian [11].

2.1.4 Algoritma

Algoritma merupakan serangkaian instruksi yang memberitahu komputer bagaimana mengubah satu set fakta tentang dunia menjadi informasi yang berguna [12]. Algoritma tidak hanya digunakan untuk menyelesaikan masalah pada komputer, tetapi juga dapat digunakan untuk menyelesaikan masalah yang ada dalam kehidupan sehari-hari. Selain itu, masalah apa pun yang terkait dengan proses atau langkah prosedural biasanya memerlukan algoritma.

2.1.5 *Support Vector Machine (SVM)*

Support Vector Machine (SVM) adalah sebuah algoritma pembelajaran mesin terawasi yang digunakan untuk klasifikasi data [13]. SVM bekerja dengan cara mencari garis atau hiperbidang (dalam dimensi yang lebih tinggi)

yang dapat memisahkan data menjadi dua kelas atau lebih dengan margin (jarak) yang sebesar-besarnya. Garis atau hiperbidang ini dikenal sebagai *hyperplane*.

2.1.6 Deteksi

Dalam Kamus besar Bahasa Indonesia deteksi adalah usaha menemukan dan menentukan keberadaan, anggapan, atau kenyataan [14], sehingga dalam penelitian ini deteksi serangan DDoS adalah menemukan serangan DDoS dalam jaringan IoMT.

2.2 Penelitian Terdahulu yang Relevan

Tabel berikut menunjukkan penelitian yang relevan dengan penelitian yang sedang penulis lakukan.

Tabel 2. 1 Penelitian Relavan

Author & Year	Method	Result
A. Binbusayyis et al. [15] (2022)	NB, DT, KNN, MLP, SVM	Model IDS yang dibuat memiliki kinerja yang baik. Namun, penelitian ini tidak menggunakan dataset khusus untuk jaringan IoMT, sehingga menimbulkan keraguan tentang keandalan model IDS yang dihasilkan.
P. Kulshrestha et al. [16] (2023)	MNB, LR, LRSGD, LSVC, DT, EVC, BG, RF, GBC, XGB, and ADB	Penelitian ini membandingkan banyak algoritma pembelajaran mesin untuk menemukan model IDS terbaik. Model IDS terbaik dihasilkan dengan menggunakan algoritma *Adaptive Boosting*. Penelitian ini tidak menggunakan dataset

		IoMT dalam melatih model IDS.
U. Zukaib et al. [17] (2024)	Meta-Learning	Penelitian ini menyajikan hasil penelitian dengan menggunakan metode meta-learning untuk membangun model IDS dengan hasil yang baik dalam mendeteksi gangguan, dataset yang digunakan pada penelitian ini adalah WUSTL-IIOT-2021, IoTID20 dan WUSTL-EHMS-2020 dataset tersebut dibangkitkan dari perangkat IoT secara umum dan IoMT. Namun, perangkat yang digunakan pada dataset IoMT pada penelitian paper ini memiliki jenis dan tipe perangkat yang kurang beragam jika dibandingkan dengan dataset yang digunakan penulis sehingga keragaman data pada dataset pada penelitian penulis lebih variatif sehingga akan menghasilkan model IDS yang lebih handal karena media untuk melatih model IDS memiliki data yang lebih variatif.
Z. Sun et al. [18] (2024)	PSO-AdaBoost	Model IDS yang dibuat memiliki performa yang baik, Namun, penelitian ini menggunakan dataset NSL KDD untuk membuat model IDS dimana dataset ini berisi data jaringan komputer secara umum, bukan jaringan IoT atau bahkan IoMT

Dari penelitian relevan yang sudah penulis jabarkan maka penulis akan menggunakan SVM untuk men erangan DDoS pada jaringan IoMT.

2.3 Kerangka Berfikir

Rumusan Masalah	Bagaimana Algoritma SVM Dengan *Kernel Polynomial* Dapat Digunakan Untuk Membuat Model IDS Untuk Deteksi Serangan DDoS Pada Dataset CICIoMT 2024.
Tujuan Penelitian	Untuk Membuat Model IDS Dengan Algoritma SVM
Metode	*Support Vector Machine* Dengan *Kernel Polynomial*
Pengukuran	*Accuracy, Precision, Recall,* Dan *F1-Score*
Capaian	Metode Yang Effisien Dalam Melakukan Klasifikasi Serangan DDoS Pada Dataset CICIoMT 2024

Gambar 2. 1 Kerangka Berfikir

BAB III
METODOLOGI PENELITIAN

3.1 Metode Penelitian

Dalam bab ini, kami menggunakan metode penelitian kuantitatif yang digunakan untuk menyelidiki penggunaan metode *Machine Learning* pada dataset CICIoMT 2024 [19]. Penelitian ini akan mulai dengan membahas data yang digunakan, diikuti dengan metode *Support Vector Machine (SVM)* dengan kernel Polynomial.

Dalam penelitian tugas akhir ini penulis menggunakan dataset CICIoMT 2024 kemudian menerapkan algoritma *Support Vector Machine (SVM)* dengan *kernel Polynomial* untuk melakukan klasifikasi data normal dan serangan pada dataset CICIoMT 2024. Performa klasifikasi akan diukur berdasarkan nilai *accuracy, recall, precision dan F1-Score.*

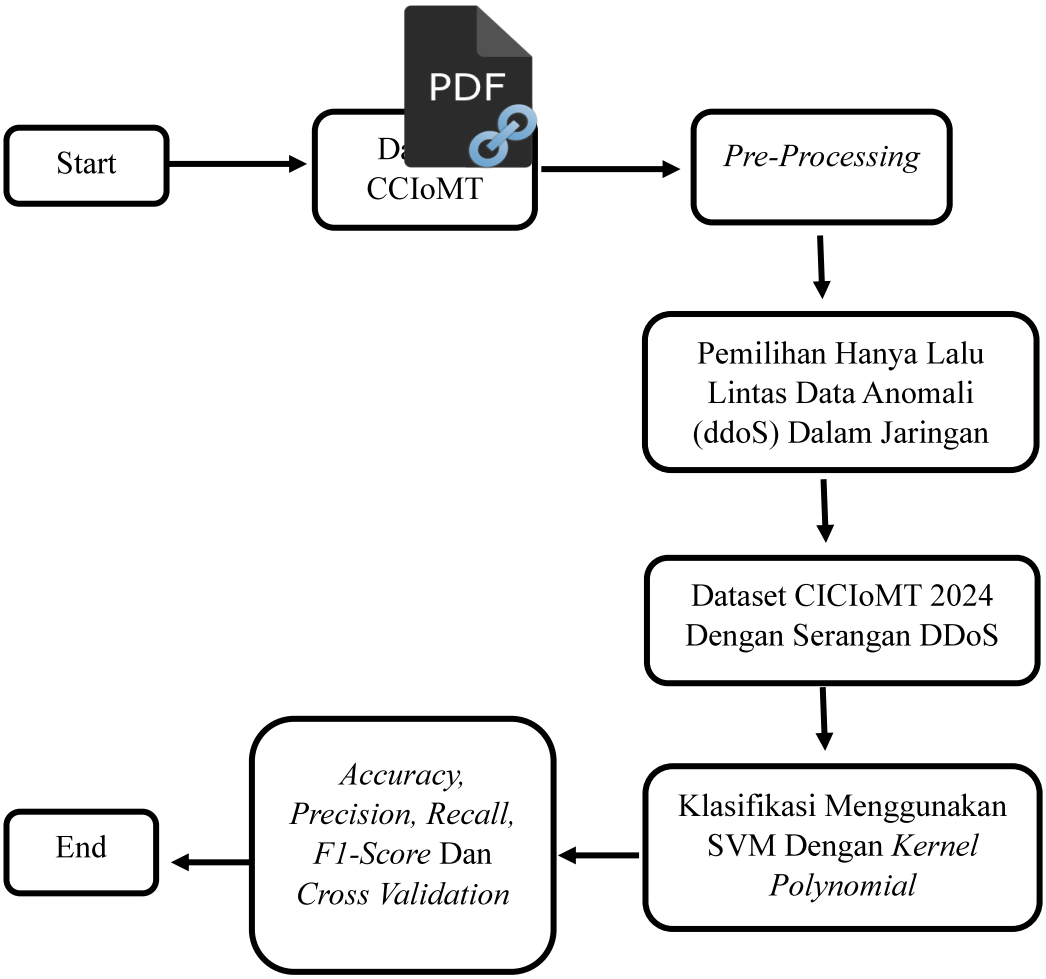
3.2 Metode Pengumpulan Data

Penelitian ini diawali dengan Observasi untuk mencari dataset yang sesuai dan dapat digunakan dalam penelitian ini, selanjutnya dilakukan studi Pustaka (studi lieteratur) kemudian mencari dan mengolah dataset. Metode pengumpulan data adalah teknik atau cara yang dilakukan oleh peneliti untuk mengumpulkan data [20]. Pengumpulan data dilakukan untuk memperoleh informasi yang dibutuhkan dalam rangka mencapai tujuan penelitian. Sementara itu instrumen pengumpulan data merupakan alat yang digunakan untuk mengumpulkan data.

Dalam penelitian ini data yang digunakan adalah dataset dari CICIoMT 2024 dalam format CSV. C 2024 adalah kumpulan data lalu lintas IoT yang dihasilkan dalam jari berukuran sedang [5]. Dataset mencakup data lalu lintas jaringan, log perangkat, dan konfigurasi perangkat. Data diberi label, sehingga dapat digunakan untuk melatih model *Machine Learning* untuk deteksi serangan. Dataset CICIoMT 2024 difokuskan pada tahap awal penyebaran botnet dan komunikasi C&C. Kumpulan data mencakup fitur-fitur seperti alamat IP, cap waktu, panjang paket, dan muatan. Kumpulan data juga diberi label, sehingga dapat diketahui lalu lintas mana yang jinak dan mana yang berbahaya. Dataset CICIoMT 2024 tersedia untuk diunduh dari situs web CIC.

3.3 Metode Analisa

Metode analisis yang digunakan dalam penelitian ini adalah metode analisis anomali adalah salah satu metode yang paling umum digunakan untuk mendeteksi serangan jaringan. Metode ini bekerja dengan mengidentifikasi perilaku atau aktivitas yang tidak biasa dalam lalu lintas jaringan. Perilaku atau aktivitas yang tidak biasa ini dapat berupa peningkatan jumlah permintaan koneksi dari sumber yang tidak dikenal, peningkatan jumlah lalu lintas dari sumber yang tidak dikenal. Gambar 2 berikut menunjukkan tahapan yang dilakukan untuk menyelesaikan penelitian tugas akhir ini.



Gambar 3. 1 Tahapan proses pembuatan model *machine learning* menggunakan algoritma SVM

Peneitian ini menggunakan dataset CICIoMT 2024 kemudian menggunakan melatih model machine learning yang dibuat menggunakan algoritma *Support Vector Machine (SVM)* dengan *kernel Polynomial*. Untuk mengukur performa dari model yang dibuat dalam mendeteksi serangan botnet dalam dataset adalah dengan mengukur *Accuracy, Precision, Recall, F1-Score Dan Cross Validation*. Hasil pengukuran ini dapat menunjukkan performa dari model yang dibuat.

3.4 Tempat dan Waktu Peneli

3.4.1 Tempat Penelitian

Tempat pene dilakukan di Ruangan Kampus B, Lab Rekayasa Sistem Komputer Universitas 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

Penelitian ini dilakukan mulai dari September 2024 dengan mengumpulkan literatur untuk memahami metode, Teknik dan data yang akan digunakan dalam peneltian ini. Penelitian ini ditargetkan selesai pada bulan januari 2024.

Tabel 3. 1 Waktu penelitian

Kegiatan	2024																2025			
	September				Oktober				November				Desember				Januari			
Minggu ke -	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
Studi Literatur																				
Analisa kebutuhan																				
Penulisan proposal																				
Bimbingan Proposal																				
Ujian Proposal																				
Penulisan Skripsi																				
Bimbingan Skripsi																				
Ujian Skripsi																				

3.5 Alat dan Bahan

3.5.1 Alat

Adapun alat yang di penulis dalam penelitian ini adalah sebagai Berikut:

1. Alat tidak habis pakai

- Laptop
- Google Colab
- Printer
- Dataset CICIoMT 2024
- Artikel Ilmiah dan Web

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 untuk mendeteksi serangan pada dataset CICIoMT 2024 dengan machine learning menggunakan *Support Vector Machine (SVM)* dengan *kernel Polynomial* adalah dengan mengukur performa model machine leraning menggunakan data test. Performa yang diukur adalah *accuracy*, *precision, recall,* dan *f1-score.*

3.6.2 Pengolahan Data

1. **Mengambil dataset [illegible]MT 2024**

   Langkah pertama [illegible]ang digunakan merupakan kumpulan data yang harus mencakup [illegible]as yang jinak dan berbahaya. Lalu lintas jinak dapat dikumpulkan dari berbagai sumber termasuk dari dataset publik (terbuka). Dalam penelitian ini menggunakan dataset CICIoMT 2024 yang dihasilkan oleh *Canadian Institute of Cybersecurity (CIC)* menggunakan *testbed* jaringan IoMT.

2. **Latih model**

   Langkah selanjutnya ketiga model *machine learning* tersebut dapat dilatih menggunakan dataset data lalu lintas jaringan yang telah diproses sebelumnya dengan algoritma pemilihan fitur. *Support Vector Machine (SVM)* dengan *kernel Polynomial*.

3. **Mengklasifikasikan Data**

   Setelah ketiga model dilatih, Anda dapat menggunakannya untuk mengklasifikasikan data lalu lintas jaringan sebagai jinak atau berbahaya. Ini dapat dilakukan dengan memasukkan data lalu lintas jaringan ke dalam model dan kemudian membandingkan hasilnya.

4. **Evaluasi model**

   Performa ketiga model tersebut dapat dievaluasi dengan membandingkan *accuracy, Precision, Recall dan F1-Score*. Evaluasiakan mencakup *Confusion matrix* bisa dilihat pada tabel berikut[21].

Tabel 3. 2 *Confussion Matrix*

Prediksi	Ac ues	
	1 (	0 *(Negative)*
	TP *(True Positive)*	FP *(False Positive)*
	FN *(False Negative)*	TN *(True Negative)*

a. *True Positives* (TP): Ini adalah contoh yang diklasifikasikan dengan benar sebagai positif.

b. *False Positive* (FP): Ini adalah contoh yang salah diklasifikasikan sebagai positif.

c. *True Negatives* (TN): Ini adalah contoh yang diklasifikasikan dengan benar sebagai negatif.

d. *False Negative* (FN): Ini adalah contoh yang salah diklasifikasikan sebagai negatif. Yang kemudian akan digunakan untuk menghitung berbagai metrik lainnya guna mengukur performa dalam mendeteksi serangan dalam dataset CICIoMT2024, seperti :

1. *Accuracy*

Accuracy adalah ukuran seberapa baik model memprediksi kelas sebenarnya dari data uji. Akurasi dihitung dengan membagi jumlah prediksi yang benar dengan total jumlah prediksi.

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

2. *Precision*

*Precis*alah ukuran seberapa baik model memprediksi positif dengan benar. Presisi dihitung dengan membagi jumlah prediksi positif yang benar dengan total jumlah prediksi positif.

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

3. *Recall*

Recall adalah ukuran seberapa baik model mendeteksi kelas positif. Sensitivitas dihitung dengan membagi jumlah prediksi positif yang benar dengan total jumlah kelas positif.

$$\text{Sensitivitas} = \frac{TP}{TP+FN} \quad \text{.....(3)}$$

4. *F1-Score*

F1 Score (F Measure) adalah ukuran seberapa baik model memprediksi kelas negatif dengan benar. Spesifisitas dihitung dengan membagi jumlah prediksi negatif yang benar dengan total jumlah kelas negatif.

$$\text{Spesitisitas} = \frac{TN}{TN+FP} \quad \text{..... (4)}$$

5. *Validasi K-Fold*

Validasik-fold ac nik validasi yang membagi data menjadi k kumpulan yang sam kumpulan digunakan sebagai kumpulan validasi satu kali, sedangkan kumpulan sisanya digunakan sebagai kumpulan pelatihan.Validasi *overfitting* dan *underfitting* adalah teknik validasi yang digunakan untuk mengatasi masalah ketidakseimbangan kelas dalam data.

BAB IV
HASIL PENE[illegible] DAN PEMBAHASAN

4.1 Gambaran Umum

4.1.1 Performa Model SVM dengan *kernel Polynomial*

Penelitian ini menggunakan algoritma *Support Vector Machine* dengan *kernel polynomial* untuk membuat model *machine learning* yang digunakan untuk mendeteksi serangan pada dataset CICIoMT 2024. Tabel 4.1 berikut menunjukkan hasil performa model *machine learning* menggunakan algoritma SVM dengan *kernel polynomial* menggunakan data latih dan 4.2 performa model yang di uji menggunakan data uji.

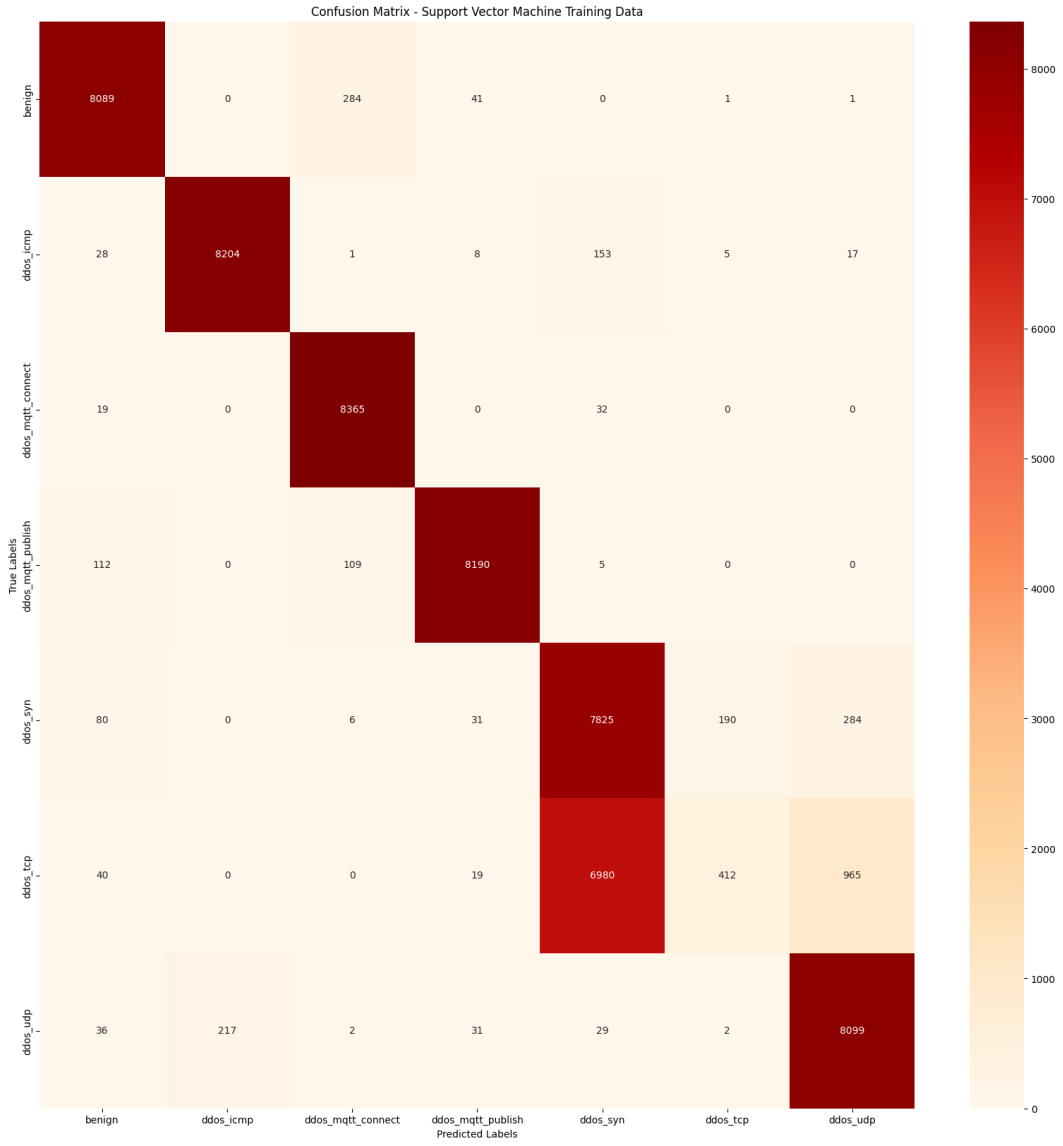
Tabel 4. 1 Performa model algoritma SVM *kernel Polynomial* pada data latih

Class	Precision	Recall	F1-Score	Accuracy
benign	0.96	0.96	0.96	83%
ddos_icmp	0.97	0.97	0.97	
ddos_mqtt_connect	0.95	0.99	0.97	
ddos_mqtt_publish	0.98	0.97	0.98	
ddos_syn	0.52	0.93	0.67	
ddos_tcp	0.68	0.05	0.09	
ddos_udp	0.86	0.96	0.91	

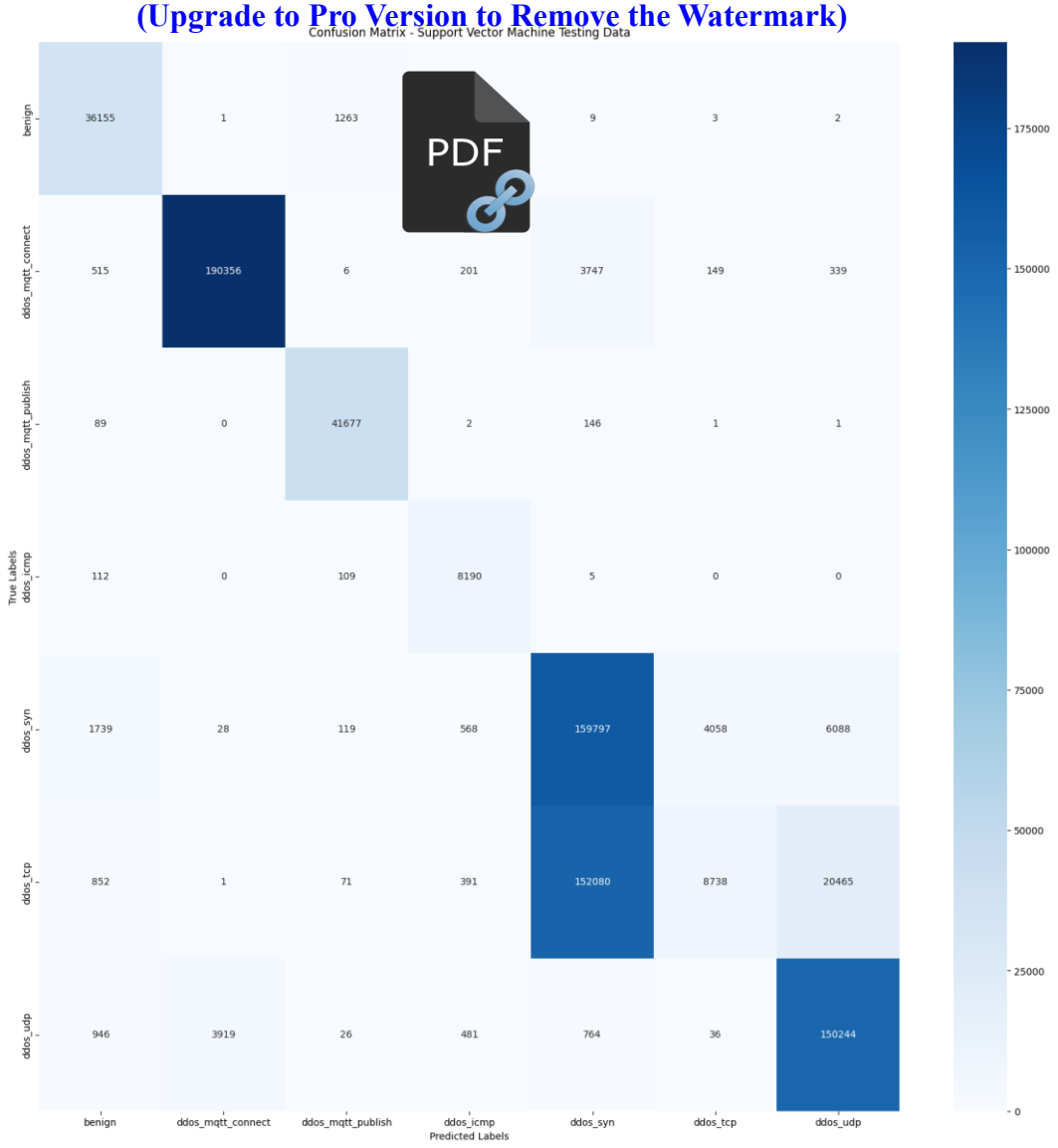
Tabel 4. 2 Performa model algoritma SVM kernel Polynomial pada data uji

Class	Precision	Recall	F1-Score	Accuracy
benign	0.89	0.96	0.93	75%
ddos_icmp	0.98	0.97	0.98	
ddos_mqtt_connect	0.96	0.99	0.98	
ddos_mqtt_publish	0.82	0.97	0.89	
ddos_syn	0.50	0.93	0.65	
ddos_tcp	0.67	0.05	0.09	
ddos_udp	0.85	0.96	0.90	

Hasil dari *confusion matrix* yang menunjukkan performa model dalam mengklasifikasikan serangan d taset ditunjukkan pada gambar 4.1 untuk data latih dan gambar 4.2 untuk kan performa model pada data uji.



Gambar 4. 1 Hasil *confusion matrix* pada data latih menggunakan algoritma SVM dengan *kernel Polynomial*

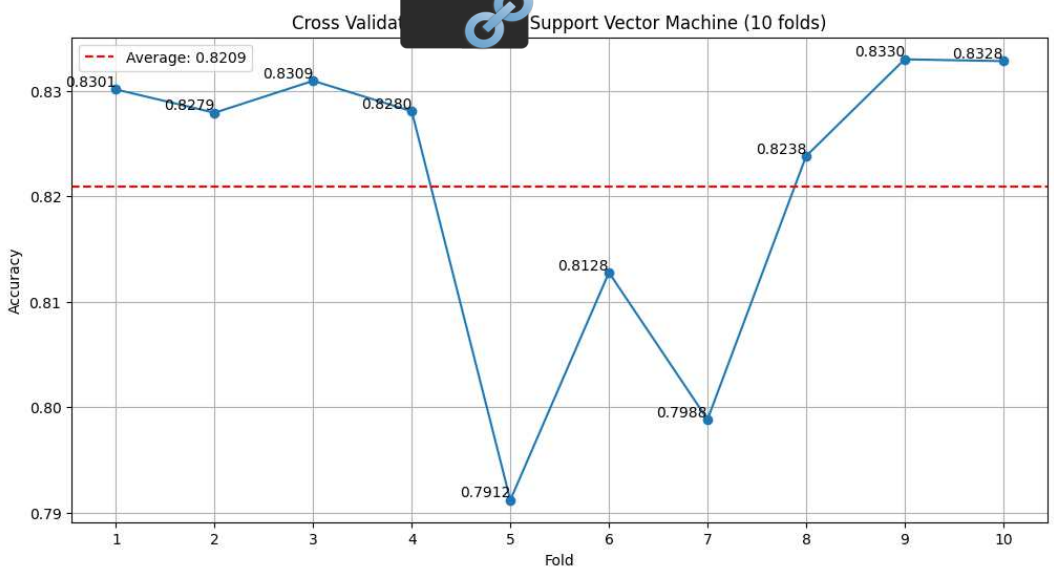


Gambar 4. 2 Hasil *confusion matrix* pada data uji menggunakan algoritma SVM dengan *kernel Polynomial*

4.1.2 Validasi model SVM dengan *kernel Polynomial*

Validasi model yang dibangun menggunakan *machine learning* penting dilakukan untuk melihat apakah model yang dibangun terdapat *overfitting*, dalam penelitian ini dalam melakukan validasi model penulis menggunakan metode *cross-validation* dengan *10-fold* untuk mengukur tingkat *overfitting* pada model yang

dibuat. Gambar 4.3 berikut menunjukkan hasil validasi model SVM dengan *kernel polynomial* menggunakn *cross-* dengan *10 fold*.



Gambar 4. 3 Hasil *cross validation* dengan 10 fold pada model SVM dengan *kernel Polynomial*

4.2 Pembahasan

4.2.1 Analisa Model SVM dengan *kernel Polynomial*

Model yang dibangun menggunakan algoritma *Support Vector Machine (SVM)* dengan *kernel polynomial* menunjukkan performa yang baik dalam mengklasifikasikan sebagian besar kelas, berdasarkan hasil evaluasi pada data latih dan data uji. Berdasarkan tabel hasil evaluasi dan gambar validasi model.

Pada data latih, model mencapai akurasi keseluruhan sebesar 83%, dengan performa terbaik pada kelas benign, ddos_icmp, dan ddos_mqtt_publish, di mana *precision, recall, dan f1-score* untuk masing-masing kelas mencapai nilai ≥0.96. Hal ini menunjukkan bahwa model mampu mengenali pola-pola serangan dari kelas-kelas tersebut dengan sangat baik. Namun, kelemahan model terlihat pada

kelas ddos_tcp, yang hanya memiliki *f1-score* sebesar 0.09, disebabkan oleh *recall* yang sangat rendah, yaitu 0.05 mengindikasikan bahwa model kesulitan mendeteksi sampel dari kelas itu, meskipun kelas ddos_syn memiliki recall yang tinggi (0.93), nilai precision-nya hanya 0.52, sehingga menghasilkan f1-score yang sedang (0.67).

Ketika diuji pada data uji, akurasi model menurun menjadi 75%, menunjukkan adanya sedikit penurunan generalisasi model terhadap data yang belum pernah dilihat sebelumnya. Sama seperti pada data latih, performa terbaik tetap dicapai pada kelas benign, ddos_icmp, dan ddos_mqtt_publish, dengan *f1-score* masing-masing ≥0.89. Namun, performa pada kelas ddos_tcp tetap rendah, dengan *f1-score* sebesar 0.09, yang konsisten dengan hasil pada data latih. Penurunan *f1-score* juga terlihat pada kelas ddos_syn, yang menurun menjadi 0.65, mencerminkan bahwa model kurang andal dalam menangani beberapa kelas tertentu pada data uji.

Hasil *confusion matrix*, seperti yang ditampilkan pada Gambar 4.1 (data latih) dan Gambar 4.2 (data uji), memberikan gambaran jumlah kesalahan klasifikasi untuk setiap kelas. Berdasarkan visualisasi tersebut, sebagian besar kesalahan klasifikasi kemungkinan terjadi pada kelas dengan *f1-score* yang rendah, seperti ddos_tcp.

4.2.2 Analisa hasil Validasi model SVM dengan *Kernel Polynomial*

Validasi model menggu ode 10-fold cross-validation, seperti yang ditampilkan pada Gambar 4.3, n n evaluasi yang lebih mendalam terhadap kemampuan generalisasi model. Metode ini memastikan bahwa setiap subset data digunakan sebagai data uji dan data latih secara bergantian, sehingga evaluasi performa menjadi lebih representatif.

Distribusi akurasi pada setiap fold menunjukkan bahwa model memiliki variasi yang kecil, yang mencerminkan stabilitas model dalam melakukan klasifikasi pada subset data yang berbeda. Meskipun demikian, perbedaan akurasi antara data latih (83%) dan data uji (75%) mengindikasikan adanya sedikit overfitting, di mana model terlalu terlatih pada data latih sehingga mengalami sedikit penurunan performa pada data uji.

BAB V
KESIMPULAN DAN SARAN

5.1 Kesimpulan

Berdasarkan hasil penelitian dapat disimpulkan bahwa algoritma *Support Vector Machine (SVM)* dengan *kernel polynomial* memiliki performa yang baik dalam mendeteksi sebagian besar jenis serangan pada jaringan, khususnya pada kelas-kelas seperti benign, ddos_icmp, dan ddos_mqtt_publish. Model ini menunjukkan nilai *precision, recall, dan f1-score* yang tinggi pada kelas-kelas tersebut, baik pada data latih maupun data uji. Akurasi keseluruhan model pada data latih sebesar 83% dan pada data uji sebesar 75%, menunjukkan bahwa model memiliki kemampuan generalisasi yang cukup baik.

Namun, penelitian ini juga mengidentifikasi kelemahan model, terutama pada kelas ddos_tcp dan ddos_syn, yang memiliki nilai *f1-score* rendah. Hal ini disebabkan oleh rendahnya *recall* untuk kelas tersebut, yang mengindikasikan bahwa model kurang mampu mengenali serangan dengan karakteristik tertentu. Selain itu, penurunan akurasi pada data uji dibandingkan dengan data latih menunjukkan adanya sedikit *overfitting* pada model.

Validasi model menggunakan metode *10-fold cross-validation* memberikan hasil yang stabil, dengan variasi akurasi antar-fold yang kecil. Hal ini menunjukkan bahwa model cukup konsisten ketika diuji pada subset data yang berbeda, meskipun masih ada ruang untuk meningkatkan generalisasi model, khususnya pada kelas dengan performa rendah.

5.2 Saran

Berdasarkan hasil penelitia beberapa saran yang dapat diberikan untuk pengembangan dan penelitian l t adalah sebagai berikut:

a. **Optimalisasi *Hyperpar*** Menggunakan teknik seperti *grid search* atau *random search* untuk mencari kombinasi parameter *kernel polynomial* yang optimal, sehingga performa model dapat ditingkatkan, terutama pada kelas dengan *f1-score* rendah.

b. **Eksplorasi *Kernel* Alternatif:** Mempertimbangkan penggunaan *kernel* lain, seperti Radial Basis Function (RBF) atau sigmoid, untuk membandingkan performa dengan *kernel polynomial*. *Kernel* alternatif ini dapat membantu meningkatkan deteksi kelas yang sulit.

c. **Penanganan Ketidakseimbangan Data:** Mengimplementasikan teknik *oversampling*, seperti *Synthetic Minority Oversampling Technique (SMOTE),* atau *undersampling* pada kelas minoritas. Pendekatan ini diharapkan dapat meningkatkan performa model pada kelas yang memiliki jumlah data lebih sedikit.

d. **Peningkatan Ekstraksi dan Seleksi Fitur:** Menggunakan metode seleksi fitur yang lebih canggih atau menambahkan fitur baru yang relevan, sehingga model dapat lebih efektif dalam mengenali pola-pola kompleks dari data.

e. **Evaluasi dengan Dataset Lain:** Menguji model pada dataset lain yang memiliki karakteristik berbeda untuk mengetahui robustitas dan kemampuan generalisasi model terhadap berbagai jenis data jaringan.

f. **Implementasi dalam Sistem Nyata:** Mengintegrasikan model yang telah dibangun ke dalam sis[illegible]ksi intrusi jaringan (IDS) untuk menguji performa model dalam[illegible]gan nyata. Hal ini akan memberikan gambaran lebih nyata tentang keandalan model.

Dengan mengikuti saran-saran ini, diharapkan performa model dapat ditingkatkan lebih lanjut, sehingga mampu mendeteksi berbagai jenis serangan jaringan dengan lebih akurat dan andal. Penelitian ini juga dapat menjadi landasan bagi pengembangan metode deteksi intrusi yang lebih canggih di masa mendatang.

DAFTAR PUSTAKA

[1] F. Ahamed and F. Farid, "App rnet of things and machine-learning for personalized healthcare: Issue allenges," *Proceedings - International Conference on Machine Learning and Data Engineering, iCMLDE 2018*, pp. 22–29, 2019, doi: 10.1109/iCMLDE.2018.00014.

[2] A. Khanna and S. Kaur, "Evolution of Internet of Things (IoT) and its significant impact in the field of Precision Agriculture," *Comput Electron Agric*, vol. 157, no. December 2018, pp. 218–231, 2019, doi: 10.1016/j.compag.2018.12.039.

[3] M. A. S. Arifin, D. Stiawan, M. Y. Idris, and R. Budiarto, "The trends of supervisory control and data acquisition security challenges in heterogeneous networks," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 22, no. 2, pp. 266–275, 2021, doi: 10.11591/ijeecs.v22.i2.pp266-275.

[4] F. B. Setiawan and Magfirawaty, "Securing Data Communication Through MQTT Protocol with AES-256 Encryption Algorithm CBC Mode on ESP32-Based Smart Homes," *2021 International Conference on Computer System, Information Technology, and Electrical Engineering, COSITE 2021*, no. October, pp. 166–170, 2021, doi: 10.1109/COSITE52651.2021.9649577.

[5] S. Vishnu, S. R. Jino Ramson, and R. Jegan, "Internet of Medical Things (IoMT)-An overview," *ICDCS 2020 - 2020 5th International Conference on Devices, Circuits and Systems*, no. April, pp. 101–104, 2020, doi: 10.1109/ICDCS48716.2020.243558.

[6] A. Ghubaish, T. Salman, M. Zolanvari, D. Unal, A. Al-Ali, and R. Jain, "Recent Advances in the Internet-of-Medical-Things (IoMT) Systems Security," *IEEE Internet Things J*, vol. 8, no. 11, pp. 8707–8718, 2021, doi: 10.1109/JIOT.2020.3045653.

[7] S. S. and A. A. G. S. Dadkhah, E. C. P. Neto, R. Ferreira, R. C. Molokwu, "CICIoMT2024: Attack Vectors in Healthcare devices-A Multi-Protocol Dataset for Assessing IoMT Device Security," *journal of Computer Communications*, 2024, doi: 10.20944/preprints202402.0898.v1.

[8] C. S. Park and H. M. Nam, "Security Architecture and Protocols for Secure MQTT-SN," *IEEE Access*, vol. 8, pp. 226422–226436, 2020, doi: 10.1109/ACCESS.2020.3045441.

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

[10] H. Le, Q. Ngo, and V. Le, "Iot Botnet Detection Using System Call Graphs and One-Class CNN Classification," *International Journal of Innovative Technology and Exploring Engineering*, no. 10, pp. 937–942, 2019, doi: 10.35940/ijitee.j9091.0881019.

[11] Liputan 6, "Pengertian Klasifik Pengelompokkan Sesuatu, Ini Penjelasan Ahli dan Contohnya." [Online]. Available: https://www.liputan6.com/hot/read/4946464/pengertian-klasifikasi-adalah-pengelompokkan-sesuatu-ini-penjelasan-ahli-dan-contohnya

[12] Gramedia, "Algoritma: Pengertian, Sejarah, Jenis, Fungsi, dan Contohnya".

[13] M. Mohammadi *et al.*, "A comprehensive survey and taxonomy of the SVM-based intrusion detection systems," *Journal of Network and Computer Applications*, vol. 178, no. December 2020, p. 102983, 2021, doi: 10.1016/j.jnca.2021.102983.

[14] KBBI, "Deteksi." [Online]. Available: https://kbbi.web.id/deteksi

[15] A. Binbusayyis, H. Alaskar, T. Vaiyapuri, and M. Dinesh, "An investigation and comparison of machine learning approaches for intrusion detection in IoMT network," *Journal of Supercomputing*, vol. 78, no. 15, pp. 17403–17422, 2022, doi: 10.1007/s11227-022-04568-3.

[16] P. Kulshrestha and T. V Vijay Kumar, "Machine learning based intrusion detection system for IoMT," *International Journal of System Assurance Engineering and Management*, 2023, doi: 10.1007/s13198-023-02119-4.

[17] U. Zukaib, X. Cui, C. Zheng, M. Hassan, and Z. Shen, "Meta-IDS: Meta-Learning Based Smart Intrusion Detection System for Internet of Medical Things (IoMT) Network," *IEEE Internet Things J*, p. 1, 2024, doi: 10.1109/JIOT.2024.3387294.

[18] Z. Sun, G. An, Y. Yang, and Y. Liu, "Optimized machine learning enabled intrusion detection 2 system for internet of medical things," *Franklin Open*, vol. 6, no. July 2023, p. 100056, 2024, doi: 10.1016/j.fraope.2023.100056.

[19] A. Guerra-Manzanares, J. Medina-Galindo, H. Bahsi, and S. Nõmm, "MedBIoT: Generation of an IoT botnet dataset in a medium-sized IoT network," *ICISSP 2020 - Proceedings of the 6th International Conference on Information Systems Security and Privacy*, no. March, pp. 207–218, 2020, doi: 10.5220/0009187802070218.

[20] Universitas Ciputra, "Metode Pengumpulan Data dalam Penelitian." [Online]. Available: https://informatika.uc.ac.id/2016/02/2016-2-18-metode-pengumpulan-data-dalam-penelitian/#:~:text=Metode pengumpulan data adalah teknik,yang digunakan untuk mengumpulkan data.

[21] kuncahyo S. Nugroho, "confusion-matrix-untuk-evaluasi-model-pada-unsupervised-machine-learning-bc4b1ae9ae3f," 2019.

DAFTAR LAMPIRAN