BAB II

TINJAUAN PUSTAKA

2.1 Teori Dasar

Pada bagian ini, dibahas beberapa konsep dan teori yang menjadi dasar dalam penelitian. Teori teori ini bertujuan untuk mendukung pemahaman terhadap topik yang dibahas. Khususnya mengenai Malware sebagai Keamanan Jaringan yang terdiri dari beberapa teori yaitu sebagai berikut:

2.1.1 Keamanan Jaringan

Menurut (Sinaga, Irmayani, and Hasibuan 2024) Dengan globalisasi dan perkembangan teknologi informasi yang cepat saat ini, keamanan jaringan menjadi masalah yang semakin penting. Semakin banyak organisasi dan individu yang bergantung pada infrastruktur jaringan untuk kegiatan sehari-hari dan operasional bisnis, membuat keamanan informasi menjadi sangat penting. Dengan berbagai jenis serangan yang terus berkembang, seperti malware, ransomware, dan serangan phishing, ancaman keamanan jaringan semakin sering dan semakin kompleks. Akibatnya, untuk mengatasi masalah keamanan ini, diperlukan pendekatan yang lebih canggih dan responsif. Sedangkan Menurut (Purnomo et al. 2024) Konsep dan masalah keamanan jaringan komputer sangat penting. Keamanan jaringan adalah teknik yang digunakan untuk melindungi sistem komputer, perangkat, dan data dari ancaman dari dalam maupun luar jaringan pada menjaga integritas, kerahasiaan, dan aksesibilitas informasi yang dikirim melalui jaringan. Berbagai jenis serangan,

seperti serangan Distributed Denial of Service (DDoS), malware, sniffing, dan jenis intrusi lainnya, dapat membahayakan jaringan komputer. Menurut Mariusz Stawowski dalam jurnalnya yang berjudul "Prinsip-prinsip desain keamanan jaringan", tujuan utama keamanan jaringan adalah untuk melindungi sumber daya sistem dari ancaman dari luar jaringan. Keamanan komputer digunakan untuk mengontrol bahaya yang terkait dengan penggunaan komputer. Komputer yang terhubung ke jaringan adalah contoh keamanan komputer.(Alfian et al. 2024)

2.1.2 Malware

Menurut (Wanli Sitorus et al. 2021) *Malicious* Software atau sering dikenal sebagai malware merupakan sebuah *software* yang diprogram agar dapat menyusup ke sebuah sistem operasi yang dapat merusak cara kerja sistem dan bahkan digunakan untuk mencuri data-data penting pada perangkat korban. Selain itu Menurut (Putra and Komputer 2024) Malware adalah perangkat lunak berbahaya yang dirancang untuk merusak, mengganggu, atau mendapatkan akses tidak sah ke sistem komputer. Untuk itu maka diperlukan analisis untuk mendeteksi malware karena tujuan akhir dari analisis malware adalah menggambarkan secara tepat cara kerja sebuah malware. Deteksi SVM (*Support Vector Machine*) terhadap serangann malware menggunakan algoritma pembelajaran mesin yang membedakan perangkat lunak berbahaya (malware) dan perilaku perangkat lunak yang sah. Malware ada dalam berbagai bentuk *script, code, activecontent,* dan perangkat lunak.

2.1.3 Jenis jenis *Malware*

Menurut (Siddiq, Yudiastuti, and Panjaitan 2020) jenis jenis malware dibagi menjadi 8 kelompok sebagai berikut:

1. ***Backdoor*** : Kode berbahaya dipasang di komputer sehingga penyerang dapat mengakses komputer tanpa proses Otentikasi

2. ***Botne t***: mirip dengan backdoor yang memungkinkan penyerang Akses ke sistem komputer dan dapat dikendalikan oleh K&C

3. ***Downloader*** : Kode berbahaya yang bertindak sebagai pengunduh bebahaya kode lain

4. ***Information stealing*** : jenis *malware* yang mengumpulkan data korban, seperti password hashing,snifing, dan keylogger

5. ***Launcher*** : kode berbahaya yang digunakan untuk menjalankan malware lainnya

6. ***Rootkit*** : *Malware* dirancang untuk menyembunyikan malware seperti Backdoor

7. ***Scareware*** : *Malware* dirancang untuk menakut-nakuti pengguna perangkat pengguna terinfeksi virus dan kemudian diminta untuk mengunduh program tertentu seperti anti virus yang ternyata Malware

8. ***Spam- sendingmalware*** : Malware yang menginfeksi komputer lain dan mengirim spam

Sedangkan menurut (Teknik and Bangsa 2025) Jenis Malware Adalah Virus, *worm, trojan*, dan *ransomware* adalah beberapa jenis malware. Virus menyebar dengan memasukkan kode ke dalam program atau file, sementara worm dapat menyebar tanpa bantuan manusia melalui jaringan komputer. Trojan berpura-pura menjadi program bermanfaat, tetapi sebenarnya mengandung kode berbahaya. yang memiliki kemampuan untuk mencuri data atau merusak sistem. Malware, juga dikenal sebagai software berbahaya, adalah program komputer yang bertujuan untuk merusak atau mengganggu sistem, mencuri data, atau mendapatkan akses tanpa izin ke sistem Ransomware mengenkripsi data korban dan meminta tebusan untuk mendapatkan kunci dekripsi.Virus, worm, trojan, ransomware, dan jenis lainnya dari malware dapat memiliki tujuan membahayakan korban

2.2 Algoritma *Machine Learning*

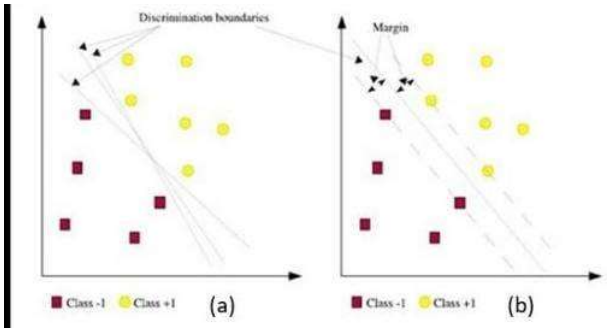
Menurut (Ningsih, Gusvarizon, and Hermawan 2022) *Machnie Learning* (ML) dalam bahasa indonesia berarti Pembelajaran Mesin, adalah suatu cabang dalam ilmu komputer yang secara umum memiliki tujuan untuk membuat program komputer yang dapat belajar dari data. Machine learning merupakan bidang multidisiplin yang artinya selain ilmu komputer, banyak ilmu-ilmu lain yang diterapkan dalam machine learning seperti statistik, matematika, logika, dan lain-lain. Sedangkan Menurut (Tjahjadi and Santoso

2023) Pembelajaran mesin, juga dikenal sebagai pembelajaran mesin, adalah ilmu komputer yang tidak diprogram secara eksplisit. Pembelajaran mesin adalah kecerdasan buatan yang mempelajari cara membuat data, dan banyak peneliti berpikir tentang bagaimana membuat kemajuan menuju AI pada skala manusia. Untuk menemukan masalah baru, teknik yang cepat dan efektif diperlukan, yang biasanya disebut pembelajaran mesin (ML). Proses pembelajaran mesin (ML) memungkinkan sistem untuk mempelajari data secara mandiri dan membuat keputusan berdasarkan pola yang ada. Proses pembelajaran mesin menggunakan algoritma matematika dan komputer untuk mengenali pola dalam data dan memprediksi hasil di masa depan.(Abdussalam and Rahmatulloh 2024)

2.2.1 *Support Vector Machine (*SVM*)*

SVM adalah algoritma pembelajaran mesin untuk klasifikasi dan regresi yang telah terbukti efektif dalam deteksi malware. Cara kerjanya adalah menemukan hyperplane optimal yang memisahkan kelas-kelas data dengan margin maksimal, menurut beberapa penelitian. Sedangkan menurut (Tjahjadi and Santoso 2023) *Support Vector Machine* (SVM) adalah algoritma pembelajaran mesin klasifikasi yang berbasis pengawasan (*Supervised Learning*). Algoritma ini menggunakan dua garis vector (*Hyperplane*) dengan margin yang terbesar. *Hyperplane* adalah garis yang digunakan untuk memisahkan data dari berbagai kelompok. Margin adalah jarak antara hyperplane dengan titik data terdekat dari masing-masing kelompok. SVM mampu menyelesaikan masalah klasifikasi baik yang bersifat linear maupun

non-linear. Algoritma SVM sudah berkembang sejak tahun 1960 dan dipresentasikan kembali oleh Boser, Vapnik, dan Guyon pada tahun 1992. SVM memiliki performa yang baik dalam berbagai bidang ilmu pengetahuan. Prinsip dasar *Support Vector Machine* adalah linear *classifier*, yang selanjutnya dikembangkan dengan mengintegrasikan konsep core trick ke dalam ruang kerja berdimensi tinggi untuk penanganan masalah nonlinier Saat ini, Support Vector Machine berhasil diterapkan pada masalah nyata dan secara umum memberikan solusi yang lebih baik daripada metode tradisional seperti jaringan syaraf tiruan. Konsep Support Vector Machine (SVM) dapat dijelaskan secara sederhana dengan mencoba mencari hyperplane terbaik yang berperan sebagai pemisah antara dua class pada input space Nazaruddin Safaat H, Aplikasi Berbasis Android. Penerbit 50 Informatika. Bandung (2013). Proses pengoperasian SVM ditunjukkan pada Gambar 2.1



Gambar 2. 1 Proses *Support Vector Machine*

Gambar 2.1 memperlihatkan beberapa model yang tergabung dalam dua kelas, yaitu: Kelas +1 dan Kelas -1. Pola kelas -1 dilambangkan dengan kotak merah, sedangkan pola kelas +1 dilambangkan dengan lingkaran kuning. Masalah

klasifikasi dapat diartikan sebagai menemukan garis (hyperplane) yang memisahkan dua kelas. Ada beberapa garis pemisah (garis pembeda), garis pemisah yang terbaik sudah cukup. Hyperplane pembeda terbaik antara kedua kelas ditemukan dengan mengukur tepi hyperplane dan mencari titik maksimum. Margin adalah jarak antara hyperplane dan pola terdekat dari setiap kelas. Pola yang memotong garis pemisah disebut vektor pendukung. Garis tengah pada gambar 2.1 menunjukkan hyperplane terbaik, yang berada tepat di tengah kedua kelas. Menemukan lokasi hyperplane ini merupakan inti dari pembelajaran SVM.

2.2.2 Metode *K-Nearest Neighbors* (*KNN*)

Menurut (Cahyanti, Rahmayani, and Husniar 2020). Algoritma *K-Nearest Neighbor* (K-NN) adalah metode klasifikasi sekumpulan data yang didasarkan pada pembelajaran data yang sudah terklasifikasikan sebelumnya. Ini termasuk dalam pembelajaran yang diawasi, di mana hasil pertanyaan instan baru diklasifikasikan berdasarkan mayoritas kedekatan jarak dari kategori yang ada dalam K-NN. Sedangkan Menurut (Halim and Anraeni 2021) Algoritma *K-Nearest Neighbor* (K-NN) adalah algoritma klasifikasi yang bergantung pada kedekatan suatu data dengan data lain. Dengan data berdimensi q, jarak antara dua data dapat dihitung. Nilai jarak ini digunakan untuk menentukan seberapa dekat atau mirip data uji dengan data latih. Nilai K pada K-NN menunjukkan K-data uji terdekat. Algoritma klasifikasi K-Nearest Neighbor digunakan untuk membuat sistem pendeteksi penyakit jantung yang efektif dan akurat.

2.2.3 Metode *Random Forest*

Menurut (Arisusanto, Suarna, and Dwilestari 2023) Random Forest adalah pengembangan dari metode *Decision Tree* yang menggunakan beberapa *Decision Tree*. Setiap *Decision Tree* telah dilatih dengan sampel dan setiap atribut didistribusikan ke pohon yang dipilih dari subset atribut yang acak. memiliki beberapa kelebihan, termasuk kemampuan untuk meningkatkan akurasi dalam kasus data yang hilang dan untuk menahan keluaran, serta kemampuan untuk menyimpan data dengan efisien. mempunyai proses seleksi fitur yang dapat mengambil fitur terbaik untuk meningkatkan kinerja model klasifikasi.

2.2.4 Metode *Naive Bayes*

Menurut (Rayuwati, Husna Gemasih, and Irma Nizar 2022) memberikan penjelasan *Naive Bayes* untuk setiap kelas keputusan, yang menghitung probabilitas dengan asumsi bahwa kelas keputusan adalah benar, mengingat vektor informasi obyek. Algoritma ini menganggap bahwa atribut obyek adalah independen. Jumlah frekuensi dari "master" tabel keputusan adalah jumlah kemungkinan yang terlibat dalam pembuatan perkiraan akhir.Jika dibandingkan dengan model klasifikasi lainnya, *Naive Bayes Classifier* memiliki kinerja yang sangat baik. Sedangkan Menurut (Wibisono, Dadi Rizkiono, and Wantoro 2020) *Naive Bayes*, juga dikenal sebagai metode multinomial *naive bayes*, digunakan untuk mengklasifikasikan sekumpulan dokumen. Ilmuwan Inggris Thomas Bayes menciptakan teknik probabilitas dan statistik yang digunakan dalam algoritma ini. Metode NB

melakukan dua tahap dalam proses klasifikasi teks: tahap pelatihan dan tahap pengujian. Pada tahap pelatihan, sampel dokumen dianalisis, termasuk pemilihan kosa kata yang mungkin ditemukan dalam sampel dokumen yang dapat digunakan sebagai representasi dari dokumen tersebut. Selanjutnya, dilakukan penentuan probabilitas prior untuk setiap kategori berdasarkan sampel dokumen tersebut. Pada tahap klasifikasi, nilai kategori setiap dokumen dihitung berdasarkan kata-kata yang ditemukan dalam dokumen yang diklasifikasikan.

2.2.5 Metode *Neural Networks*

Menurut (Rayuwati et al. 2022) Menurut Haykin (2009), Jaringan Saraf Tiruan (JST) atau *Artificial Neural Network* (ANN) adalah prosesor terdistribusi besar-besaran secara paralel yang terdiri dari unit proses sederhana. ANN dapat menyimpan pengetahuan dalam bentuk pengalaman dan dapat digunakan untuk proses lain. ANN juga dapat digambarkan sebagai jaringan yang mirip dengan otak manusia yang diprogram untuk melakukan tugas tertentu. ANN dapat digunakan untuk memodelkan hubungan yang kompleks antara input dan output, yang kemudian dapat digunakan untuk menemukan pola dalam data. Biasanya, jaringan ini dijalankan dengan komponen elektronik atau disimulasikan melalui aplikasi komputer.

2.2.6 Metode *Decision Tree*

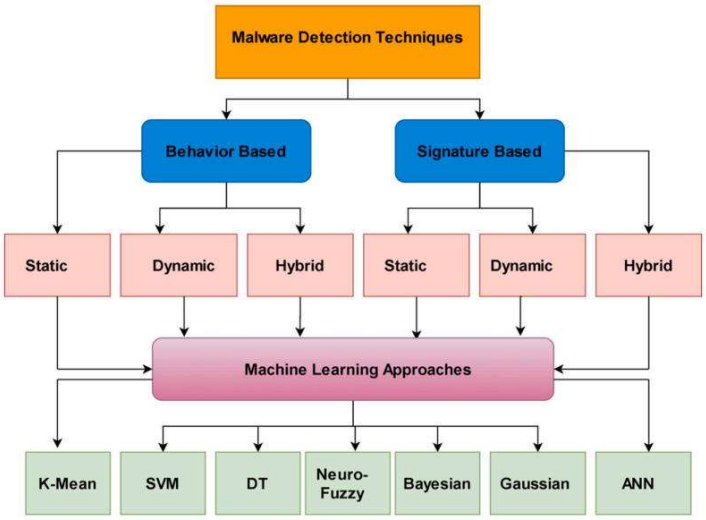
Menurut (Pertiwi, Oktavia, and Maulana 2023) *Decision Tree* adalah algoritma pembelajaran mesin yang mudah dipahami dan sering digunakan dalam penelitian keamanan jaringan. Dalam penelitian ini, *Decision Tree* diterapkan untuk

mengidentifikasi malware di dalam lingkungan komputasi awan. Decision tree membuat struktur seperti pohon keputusan yang mudah dipahami dan ditafsirkan oleh manusia. dengan baik untuk data dengan berbagai jenis fitur, seperti fitur numerik dan kategorikal. Ini membuatnya cocok untuk berbagai jenis data, termasuk data jaringan.

Sedangkan Menurut (Bintoro, Trisnawan, and Data 2023) *Decision Tree* termasuk dalam kategori machine learning dan merupakan bagian dari supervised learning. *Decision tree* juga dikenal sebagai CART (Classification and Regression Tree), dan metode ini adalah kombinasi dari dua jenis pohon: *classification tree* dan *regression tree.*

2.3 Metode Deteksi Serangan *Malware*

Metode deteksi serangan malware dapat dibagi ke dalam beberapa kategori utama berdasarkan pendekatan dan teknologi yang digunakan. Berikut ini ringkasan metode yang umum digunakan:

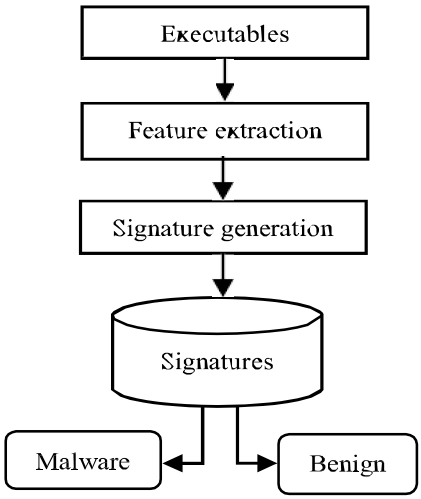


Gambar 2. 2 Metode Deteksi Serangan Malware

Menurut (Azeem et al. 2024) Berikut Metode Deteksi Serangan Malware Yang Digunakan Pada Umumnya sebagai berikut:

2.3.1 Metode *Sinagture Based Detection*

Signature adalah fitur malware yang membantu menyembunyikan struktur program dan membedakan setiap malware dengan cara yang berbeda. Antivirus yang dijual menggunakan metode pengenalan berbasis tanda. Ini mendeteksi malware yang diketahui dengan cepat dan efektif, tetapi tidak cukup untuk mendeteksi malware yang tidak diketahui. Selain itu, *malware belonging to the same family can easily avoid signature-based detection by using techniques of obfuscation.*. Berikut Gambaran umum skema pengenalan berbasis tanda.



Gambar 2. 3 Metode *Signature Based Detection*

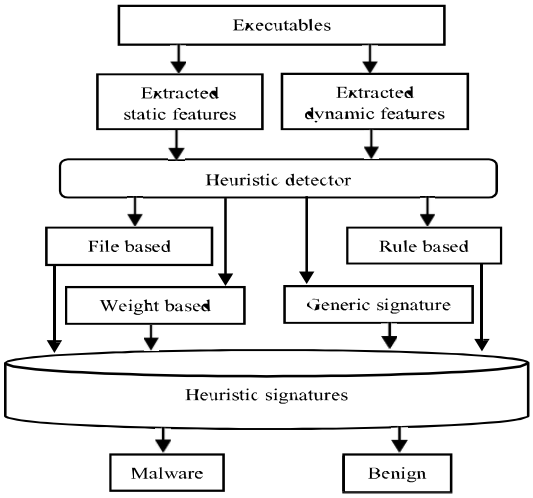
2.3.2 Metode *Heuristic-Based Detection*

Menurut (Aslan and Samet 2020) Metode deteksi berbasis heuristik telah menjadi lebih populer dalam beberapa tahun terakhir. Meskipun metode ini menggunakan pengalaman dan berbagai teknik, seperti aturan dan teknik ML, untuk mendeteksi malware zero-day, itu tidak dapat menemukan malware yang rumit. Gambar ini menunjukkan skema deteksi berbasis heuristik.

2.3.3 Metode *Behavior-Based Detection*

Menurut (Bahador, Abadi, and Tajoddin 2019) Dalam beberapa tahun terakhir, berbagai teknik analisis telah diciptakan untuk menemukan program jahat. Analisis ini terdiri dari dua kategori utama: analisis statis dan dinamis. Analisis statis menemukan pola yang mencurigakan dengan menggunakan kode sumber atau pemeriksaan berkas biner. Meskipun cepat dan efektif, metode ini memiliki beberapa keterbatasan. Hal ini terutama berlaku karena metode pengaburan dapat

dihindari dengan mudah. Oleh karena itu, teknik ini tidak dapat menemukan program jahat baru yang berbeda dari yang sudah ada. Analisis dinamis, juga dikenal sebagai teknik deteksi perilaku, telah diusulkan untuk mengatasi keterbatasan ini dan mengidentifikasi program jahat berdasarkan perilakunya. Teknik ini menjelaskan cara program jahat dan jinak berinteraksi dengan sistem operasinya. Ini termasuk menghasilkan jejak panggilan sistem dan menggunakan sumber daya sistem.



Gambar 2. 4 Metode Heuristic- Based

2.3.4 Metode *Machine Learning-Based Detection*

Menurut (Rani et al. 2022) Karena beberapa alasan, memerangi ransomware sama sekali bukan tugas yang mudah.Ransomware serupa dengan perangkat lunak yang tidak berbahaya dan beroperasi tanpa diketahui orang lain. Akibatnya, deteksi ransomware dalam serangan zero-day sangat penting saat ini. Tujuan utamanya adalah untuk mencegah ransomware merusak sistem, menemukan ransomware

zero-day (yang sebelumnya tidak terlihat) dan sebisa mungkin tidak terlihat. Ada berbagai cara untuk mengidentifikasi ransomware. Metode yang didasarkan pada analisis statis membongkar kode sumber tanpa menjalankannya.Metode ini memiliki rasio positif palsu yang tinggi dan tidak dapat menemukan ransomware yang dikaburkan. Variasi baru sering muncul, dan penyerang juga mengubah kode mereka dengan berbagai metode pengemasan. Untuk menyelesaikan masalah ini, para peneliti menggunakan pendekatan yang didasarkan pada analisis perilaku dinamis, yang melacak interaksi antara kode yang digunakan dalam lingkungan virtual. Metode deteksi ini, bagaimanapun, lebih lambat dan membutuhkan jumlah sumber daya memori yang besar.Untuk analisis perilaku proses atau aplikasi apa pun, pendekatan pembelajaran mesin adalah yang terbaik.

2.3.5 Metode *Deep Learning-Based Detection*

Menurut (Tayyab et al. 2022) Pembelajaran Mendalam adalah bentuk pembelajaran mesin khusus dalam domain Kecerdasan Buatan (AI) yang menerapkan jaringan saraf buatan dalam yang juga dikenal sebagai jaringan saraf dalam. Ini adalah teknik pembelajaran mesin yang mensimulasikan proses pembelajaran oleh otak manusia. Otak manusia terdiri dari sel-sel yang disebut sebagai neuron dalam jaringan saraf. Demikian pula, dalam otak manusia, semua sel terhubung melalui akson dan dendrit dengan wilayah koneksi yang dikenal sebagai sinapsis. Koneksi ini ketika ditemukan dalam ANN (Jaringan Saraf Buatan), mengandung bobot untuk berperilaku sebagai koneksi antara sel-sel saraf di otak manusia. Jumlah lapisan jaringan saraf dalam membedakan jaringan saraf

konvensional dari jaringan saraf dalam. Untuk abstraksi data tingkat tinggi, jaringan saraf dalam menggunakan banyak lapisan tersembunyi. Jaringan ini memiliki kemampuan untuk mempelajari fitur data, dan proses rekayasa fitur ini dilakukan dengan bantuan sejumlah besar contoh yang dimasukkan ke dalam algoritma berbasis pembelajaran mendalam. Selama proses rekayasa fitur, algoritma ini menghasilkan hasil dalam bentuk klasifikasi, identifikasi, atau pembuatan data setelah mempelajari fitur yang paling sesuai. Mengatur dan menganalisis sejumlah besar data adalah alasan utama untuk menggunakan pembelajaran mendalam di berbagai bidang. Pemrosesan gambar, pemrosesan ucapan, perawatan kesehatan, dan meningkatnya ruang siber saat ini bahkan memungkinkan penggunaan jaringan dalam.

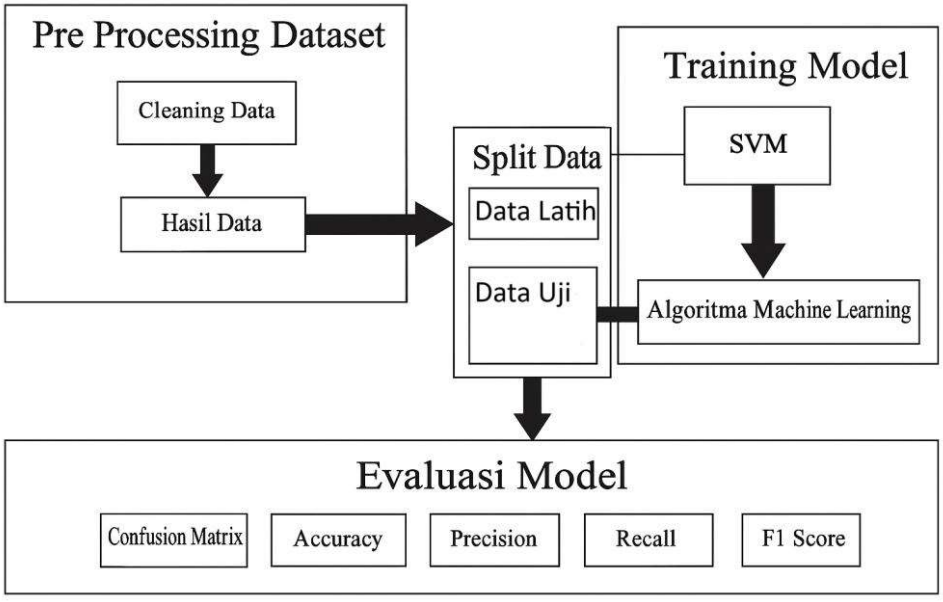
2.3.6 Metode *Hybrid Detection*

Menurut (Baek et al. 2021) mengusulkan teknik analisis hibrid untuk mendeteksi malware penambangan kripto dengan menggunakan opcode yang diekstrak dari analisis statis dan panggilan sistem yang dihasilkan dari analisis dinamis. Model LSTM, LSTM berbasis perhatian (ATT-LSTM), dan CNN, teknik pembelajaran mendalam, digunakan untuk mendeteksi malware penambangan kripto.Santos dkk. menyarankan OPEM sebagai metode hibrid untuk mendeteksi malware yang tidak diketahui. OPEP menggunakan analisis statis untuk mengekstrak urutan kode op dengan panjang tetap, dan kemudian menghasilkan vektor frekuensi. Selain itu, jejak eksekusi, seperti panggilan sistem dan operasi yang dikumpulkan melalui analisis dinamis, diubah menjadi vektor biner. Vektor

ini digunakan untuk melatih jaringan KNN, DT, SVM, NB, dan Bayesian untuk mengidentifikasi malware. Untuk melakukan deteksi malware akhir, skema 2-MaD yang diusulkan dalam penelitian ini melakukan analisis dinamis pada file yang dianggap jinak dengan menggunakan analisis statis. Tingkat deteksi malware IoT yang salah yang diklasifikasikan sebagai malware jinak meningkat secara signifikan dengan menggunakan analisis hibrid dua tahap.

2.4 Kerangka Pemikiran

Berikut ini kerangka pemikiran pada penelitian deteksi serangan malware menggunakan metode support vector machine



Gambar 2. 5 Kerangka Pemikiran

Agar dapat memahami kerangka pemikiran berikut penjelasan dari kerangka pemikiran:

1. Pre-Processing Dataset

Tahapan awal ini bertujuan untuk membersihkan data mentah yang dikumpulkan dari sumber dataset. Pembersihan data adalah proses di mana nilai yang tidak valid atau kosong dihilangkan, tipe data diubah menjadi konsisten, dan bentuk data numerik disesuaikan. Setelah langkah ini selesai, data akan dibuat dan disiapkan untuk tahap selanjutnya.

2. Split Data

Dataset yang telah dibersihkan kemudian dibagi menjadi dua bagian utama yaitu Data Pelatihan dan Data Uji. Data Pelatihan Digunakan untuk melatih model pembelajaran mesin, dan data uji, digunakan untuk mengevaluasi seberapa baik model yang telah dilatih melakukan prediksinya. Untuk menjamin bahwa evaluasi model dapat dilakukan secara objektif, pembagian ini sangat penting.

3. Training Model

Pada tahap ini, algoritma Support Vector Machine (SVM) digunakan untuk melakukan pelatihan model. Model akan belajar mengenali pola dari data yang dilatih dan kemudian membuat fungsi klasifikasi untuk membedakan antara data yang dilabelkan sebagai serangan dan yang tidak.

4. Evaluasi Model

Setelah model dilatih, fase evaluasi dilakukan dengan data uji. Berikut ini adalah beberapa metrik evaluasi yang digunakan untuk mengukur kinerja model:

1. *Confusion Matrix* digunakan untuk mengetahui berapa banyak prediksi yang benar atau salah.

2. *Accuracy*: Kapasitas model untuk memprediksi dengan benar
3. *Precision*: Ketepatan prediksi serangan model
4. *Recall*: Kemampuan model untuk menemukan data serangan secara keseluruhan.
5. *F1 Skor*: Skor precision dan recall rata-rata harmonis.

2.5 Penelitian Terdahulu

Berikut merupakan penelitian terdahulu yang didapatkan dari berbagai jurnal penelitian terkait.

Tabel 2. 1 Penelitian Terdahulu

N0	Author	Judul	Masalah	Metode	Hasil
1	(Jacobus and Winarko 2014)	Penerapan Metode Support Vector Machine pada Sistem Deteksi Intrusi secara Real-time	Dengan metode baru, sistem tidak dapat mendeteksi serangan.	Data mining dengan algoritma Decision Tree, Random Forest, dan Support Vector Machine	Hasil penelitian menunjukkan bahwa, dibandingkan dengan Decision Tree dan Support Vector Machine (SVM), metode data mining, terutama algoritma Random Forest, memiliki kinerja deteksi malware terbaik.
2	(Putra and Komputer 2024)	Analisis Data Mining Untuk Deteksi Malware Pada Jaringan Komputer	Meningkatnya penggunaan internet dan perangkat terhubung	Dalam penelitian ini, beberapa algoritma data mining seperti Decision Tree, Random Forest, dan	Hasil penelitian menunjukkan bahwa metode data mining—terutama

N0	Author	Judul	Masalah	Metode	Hasil
			jaringan menyebabkan peningkatan jumlah ancaman keamanan yang signifikan, termasuk serangan malware.	Support Vector Machine (SVM)	algoritma Random Forest— memiliki kinerja deteksi malware terbaik dibandingkan dengan Decision Tree dan Support Vector Machine (SVM).
3	(Wanli Sitorus et al. 2021)	Analisis Deteksi Malware Android menggunakan metode Support Vector Machine & Random Forest	Serangan malware dapat merugikan pengguna Android, jadi analisis malware diperlukan.	Metode Support Vector Machine Dan Metode Random Forest	Dalam hal ini, pengujian terhadap ketiga skenario yang ada menunjukkan bahwa metode Random Forest lebih unggul daripada metode SVM, dengan akurasi Random Forest sebesar 98,99%, sedangkan metode SVM menunjukkan akurasi sebesar 96,23%.
4	(Zulfikri et al. 2023)	Analisis Keamanan Jaringan Dari Serangan Malware Menggunakan	Peningkatan serangan malware, yang merusak baik	Firewall Filtering Dengan Port Blocking	Hasil penelitian ini sangat bermanfaat karena tidak

N0	Author	Judul	Masalah	Metode	Hasil
		Filtering Firewall Dengan Port Blocking	individu maupun organisasi, menyebabkan kebocoran data, gangguan operasional, dan kerugian finansial, adalah latar belakang penelitian ini.		hanya bandwidth yang memperlambat akses jaringan tetapi juga komponen lain yang dapat menyebabkan peningkatan trafik jaringan. Penelitian ini menemukan bahwa teknik seperti ini dapat digunakan untuk meminimalkan kondisi lalu lintas jaringan di perusahaan besar.
5	(Diana Dewi et al. 2023)	Perbandingan Metode Neural Network Dan Support Vector Machine Dalam Klasifikasi Diagnosa Penyakit Diabetes	Dengan diagnosis awal atau prediksi, orang diharapkan dapat menghindari atau mencegah hal-hal yang berbahaya, dalam hal ini diabetes.	Metode Neural Network Dan Support Vector Machine	Berdasarkan hasil analisis penelitian ini, metode ANN memiliki nilai akurasi 77,60%, sedangkan metode SVM memiliki nilai akurasi 65,24%. Ini menunjukkan bahwa metode ANN lebih baik dalam mengidentifikasi apakah seseorang

N0	Author	Judul	Masalah	Metode	Hasil
					menderita diabetes atau tidak.
6	(Informasi et al. 2016)	Peningkatan Keamanan jaringna terhadap serangan malware menggunakan teknik honyepot dionaea	Sistem pertahanan yang terdiri dari firewall, antivirus, dan sistem pendeteksi penyusupan dalam jaringan (juga dikenal sebagai sistem pendeteksi penyusupan jaringan/NIDS) diperlukan untuk menangani masalah keamanan jaringan tersebut.	teknik honyepot dionaea	Sistem honeypot dionaea dapat membantu sistem keamanan jaringan melawan malware.
7.	(Matin et al. 2023)	Deteksi Malware Menggunakan Machine Learning Dengan Metode Ensemble	Ancaman malware dengan perangkat lunak yang dirancang dengan tujuan negatif terus meningkat setiap tahun. Tujuannya termasuk merusak data, mencuri informasi	Menggunakan Machine Learning Dengan Metode Ensemble	Decision tree memiliki kinerja yang cukup baik dengan tingkat akurasi sebesar 93,5%. Konsistensi antara presisi dan recall juga terlihat pada angka yang hampir sama, yaitu 93%. Hutan acak lebih baik dari Decision tree dengan tingkat

N0	Author	Judul	Masalah	Metode	Hasil
			penting, mengganggu kinerja perangkat, dan mengambil alih sistem.		akurasi sebesar 94,9%.
8	(Siddiq et al. 2020)	Analisis Perilaku Malware Dengan Metode Surface Analysis Dan Runtime Analysis	Namun, hal ini juga memungkinkan orang-orang yang memiliki niat jahat untuk mengambil keuntungan secara ilegal dengan berbagai cara, seperti membuat Malware yang dimasukkan ke dalam program atau dengan cara-cara lainnya.	metode Surface Analysis dan Runtime Analysis	Karena memiliki string yang biasanya ada pada malware, File Games.exe jelas merupakan malware.
9	(Agus Syamsul Arifin et al. 2024)	Deteksi Aktifitas Malware pada Internet of Things menggunakan Algoritma Decision Tree dan Random Forest	Namun, bahaya siber, terutama malware, meningkat seiring dengan peningkatan adopsi Internet of Things. Fokus penelitian ini adalah mendeteksi	Algoritma Decision Tree dan Random Forest	Hasil pengujian menunjukkan bahwa model sistem deteksi intrusi (IDS) yang menggunakan algoritma forest random memiliki hasil yang lebih baik daripada model IDS yang

N0	Author	Judul	Masalah	Metode	Hasil
			serangan malware pada jaringan Internet of Things dengan menggunakan algoritma machine learning Decision Tree dan Random Forest.		menggunakan algoritma decision tree.
10.	(Teknik and Bangsa 2025)	Cybersecurity Untuk Menghadapi Ancaman Malware	Serangan cyber juga dapat menyebabkan ketidakpuasan, stres, dan kecemasan.	algoritma seperti Random Forest, Support Vector Machines, Convolutional Neural Networks, Recurrent Neural Networks, dan Autoencoders	Teknologi pengajaran mesin dan pengajaran mendalam telah meningkatkan deteksi malware dengan menganalisis pola perilaku yang mencurigakan.
11.	(Hilal et al. 2022)	Malware Detection Using Decision Tree Based SVM Classifier for IoT	as the increasing threat and malware attacks during the transmission of highly confidential medical data in the Internet of Medical Things (IoMT)	Method SVM	The dataset used for evaluating the proposed MLBCT-Mdetect has infected and uninfected an application which counts to 545 benign and 421 malware applications. True Positive

N0	Author	Judul	Masalah	Metode	Hasil
			environment. This is due to the rapid advancements and exploitation of smart IoT devices in healthcare technology.		Rate (TPR), false positive Rate (FPR) and Accuracy are the measures considered for evaluating the proposed scheme.
12.	(Akbar and Sutabri 2024)	Implementasi Teknologi AI Dalam Deteksi dan Pencegahan Serangan Malware pada Jaringan Komputer Perusahaan	Virus, worm, trojan, ransomware, dan jenis malware lainnya telah menjadi ancaman yang semakin meningkat dan merugikan perusahaan di seluruh dunia.	Metode machine learning dan deep learning	Sebelum menggunakan AI, perusahaan harus melakukan penilaian risiko yang menyeluruh untuk menemukan kerentanan dalam jaringan mereka. Ini akan membantu dalam menentukan area prioritas di mana AI dapat meningkatkan keamanan secara signifikan.
13.	(W et al. 2024)	Deteksi Serangan Malware Pada Web Aplikasi Menggunakan Metode Malware Analis Dinamis dan Statis	Karena dunia semakin terdigitalisasi, volume data meningkat dengan cepat. Akibatnya, banyak peretas	Metode Malware Analis Dinamis dan Metode Malware Analisis Statis	Hasil penelitian menunjukkan bahwa serangan malware dapat masuk ke jaringan dan kemudian masuk ke

N0	Author	Judul	Masalah	Metode	Hasil
			melakukan penyusupan, dan jutaan situs web terkena serangan malware yang dapat menyebabkan kerugian miliaran dolar. Struktur		webserver menggunakan metode pasif. Meskipun demikian, ketika file Exampel Malware.exe diaktifkan atau diklik, malware ini akan bekerja secara aktif dan menginfeksi sistem dan jaringan, bahkan jika administrator tidak menyadari bahwa web aplikasi dari webserver atau website tersebut telah terinfeksi.
14.	(Christodorescu et al. n.d.)	Semantics-Aware Malware Detection	The increasing threat of malware during the transmission of highly confidential medical data in the Internet of Medical Things (IoMT) environment is a major issue in this study. This issue arises due to the advancement of technology and the exploitation of smart IoT	Metode MLBCT-Mdetect	MLBCT-Mdetect processes 1000 samples in just 42 seconds, demonstrating a much higher delivery speed compared to the n-gram method across a wide range of sample sizes.

N0	Author	Judul	Masalah	Metode	Hasil
			devices in healthcare technology, which increases the risk of malware attacks.		
15	(Rani et al. 2022)	A Survey on Machine Learning-based Ransomware Detection	increasing threats and malware attacks during the transmission of highly confidential medical data in the Internet of Medical Things (IoMT) environment.	MLBCT-Mdetect	MLBCT-Mdetect achieved 98.87% accuracy in detecting malware using the Decision Tree-based SVM classifier. This figure is much higher compared to other machine learning methods tested, such as Naïve Bayes (87.78%), K-Nearest Neighbor (KNN) (85.12%), and Random Forest (80.12%).