BAB II

TINJAUAN PUSTAKA

2.1. Penelitian Terkait

2.1.1. Penelitian "Implementasi Algoritme *Support Vector Machines* untuk Klasifikasi Area Terbakar di Lahan Gambut" Oleh Edi dkk 2021

Penelitian ini menjelaskan tentang bagaimana mencari informasi mengenai luas area kebakaran di lahan gambut untuk kemudian menentukan kebijakan yang akan diambil. Metode sebelumnya dilakukan dengan teknik interpretasi visual *on screen,* sehingga membutuhkan tenaga interpreter berpengalaman. Solusinya adalah dengan membuat teknik interpretasi digital menggunakan algoritma *Support Vector Machine* dan menghasilkan klasifikasi dengan akurasi 99.8%. Relevansi laporan akhir yang dibuat dengan penelitian ini terletak pada penggunaan algoritma SVM untuk metode klasifikasi.

2.1.2. Penelitian "SCADA System Testbed for Cybersecurity Research Using Machine Learning Approach" Oleh Marcio dkk 2018

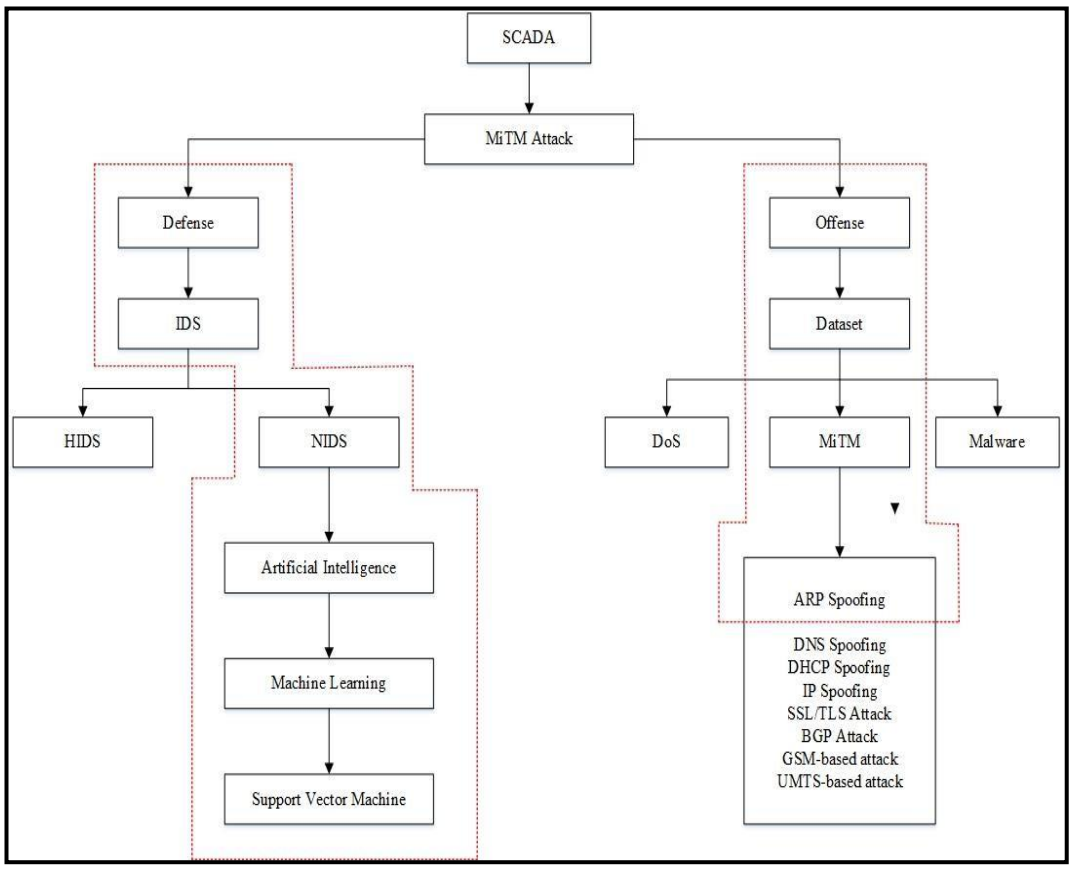
Penelitian ini memaparkan pengujian keamanan jaringan dari *Supervisory Control dan Data Acquisition* (SCADA) dengan menggunakan lima metode *machine learning* yang berbeda yaitu *Random Forest, Decision Tree, Logistic Regression, Naïve Bayes* dan KNN, kemudian membandingkan performa algoritma *machine learning* tersebut dengan cara diuji dalam jaringan *offline* dan *online.* Relevansi penelitian dengan laporan akhir terletak pada kesamaan penggunaan dataset SCADA untuk meneliti *Intrusion Detection System* berbasis *machine learning* dan menunjukan hasil keefektifannya.

2.1.3. Penelitian "Man In The Middle (MITM) Attack Detection Tool Design" Oleh Baris dkk 2018

Pada penelitian ini dijelaskan tentang karakteristik dari serangan Man In The Middle dengan tujuan untuk merancang alat deteksi serangan Man In The Middle yang sederhana, cepat, dan handal. Penelitian ini memberikan perspektif ide untuk mendeteksi serangan Man In The Middle.

2.2. Diagram Konsep Penelitian

Pada laporan akhir ini terdapat beberapa bagian atau sub materi yang akan dibahas, oleh sebab itu perlu dirancang sebuah kerangka konsep secara hirarki atau urutan untuk menampilkan pembahasan penelitian secara keseluruhan. Diagram konsep penelitian dapat dilihat pada gambar 2.1.



Gambar 2.1 Diagram Konsep Penelitian

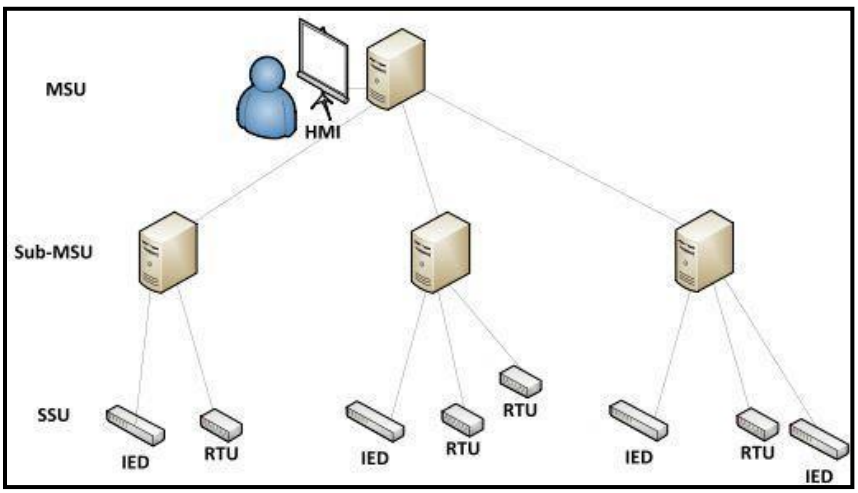
Gambar 2.1 merupakan sebuah gambaran dari diagram konsep pada penelitian, dalam gambar tersebut terdapat sisi *defense* dan *offense*, bagian yang diberi border garis titik merupakan *scope* atau cakupan dari penelitian yang akan dibahas.

2.3. Supervisory Control And Data Acquisition (SCADA)

Supervisory control and data acquisition (SCADA) system adalah jenis Industrial Control System (ICS) yang mengumpulkan data dan memonitor

otomatis di seluruh wilayah geografis yang jarak pisah nya hingga ribuan mil. System scada memungkinkan sebuah operator yang ada di lokasi pusat untuk dapat mendistribusikan secara luas, seperti ladang minyak atau gas, system pipa, system irigasi atau bahkan pembangkit listrik tenaga air yang kompleks, untuk membuat perubahan set point pada pengontrol proses yang jauh, untuk membuka atau menutup saklar, untuk memonitor alarm, dan untuk mengumpulkan informasi sebuah pengukuran.

Dalam komunikasi Scada menggunakan standar komunikasi seperti *Modbus, DNP3, Profinet, IEC-60870-5* dan *IEC-61850.* System Scada memantau dan mengendalikan proses industri yang terdistribusi secara geografis dengan perangkat kontrol seperti *Remote Terminal Unit* (RTU) dan *Master Terminal Unit* (MTU), kelancaran dan keandalan system Scada sangat penting dalam proses industri karena membutuhkan akuisisi dan kontrol data secara *realtime* (Cherdantseva, 2016).



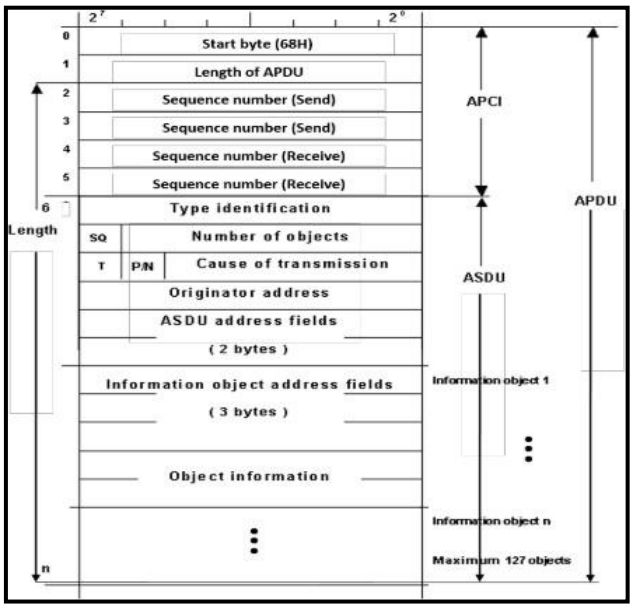
Gambar 2.2 Arsitektur Jaringan SCADA

Pada gambar 2.2 merupakan sebuah arsitektur dari jaringan scada yang biasanya memerlukan tiga jenis komunikasi, yaitu *unicast, multicast,* dan *broadcast*. Dimana Komunikasi Unicast berarti sebuah pesan yang dikirim adalah dari satu titik ke titik yang lain. Misalnya komunikasi antara MSU ke sub-MSU, dimana dari titik MSU langsung ke titik sub-MSU dinamakan komunikasi *Unicast*. Komunikasi *Multicast* berarti pesan yang dikirimkan dari satu titik ke

beberapa titik yang lain. Misalnya komunikasi antara MSU dan beberapa sub-MSU. Dan yang terakhir komunikasi *Broadcast* berarti pesan yang dikirimkan dari satu titik dikirimkan ke semua titik lainnya. Sebagai Contoh, Komunikasi antara MSU dan semua jaringan sub-MSU.

2.3.1 *Protocol IEC-60870-5-104*

Protocol IEC-60870-5-104 (IEC 104) banyak digunakan dalam system scada modern. Kerangka dasar dalam protocol *IEC-104* disebut *Protocol Data Unit (APDU)* dan kerangka *APDU* dapat menjadi menjadi format U,S atau I. *Control Frame (U)* yang tidak dinomori digunakan untuk menguji, memulai atau menghentikan aliran sebuah komunikasi. *Supervisory Format (S)* digunakan untuk melakukan fungsi pengawasan yang bernomor. *Information Instruction Format (I)* digunakan untuk mengirim perintah dan informasi yang bernomor. *Spontaneous events* atau peristiwa yang spontan seperti terjadi secara langsung hanya dapat dikirim dalam format I (Yang, 2014).



Gambar 2.3 Format Frame Tipe I

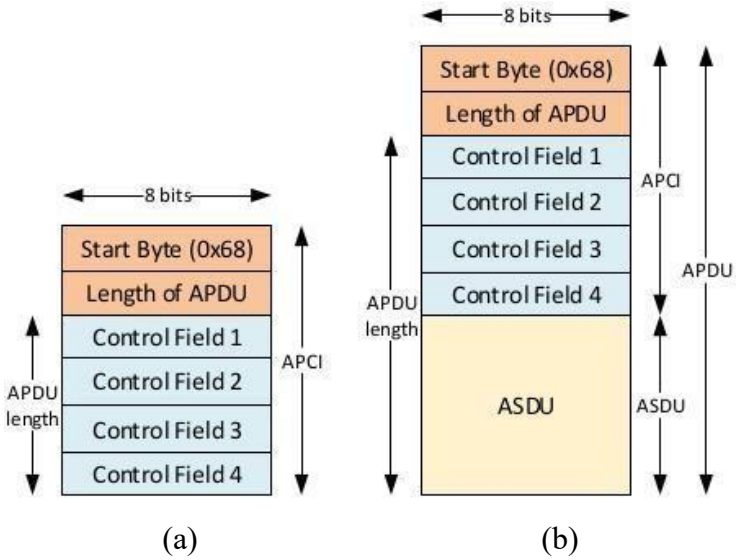
Pada Gambar 2.3 menyajikan format frame untuk paket tipe I. Format I *APDU* dibentuk dari *Application Protocol Control Information (APCI)* dan *Application Service Data Unit (ASDU)*. *APCI* berisi informasi dasar seperti

panjang paket dan nomor urut dan *ASDU* berisi atribut yang terperinci. *IEC-60870-5-101* adalah komunikasi standar untuk mengirim pesan telekontrol dasar antara RTU dan MTU mempunyai fitur komunikasi seperti:

1. *Unbalanced transmission* merupakan mode komunikasi dimana perangkat pengendali mengontrol semua lalu lintas data dengan menentukan perangkat yang dikendalikan secara berurutan, perangkat yang dikendalikan hanya bisa merespon pesan, mode ini mendukung layanan seperti *send/noreply, send/confirm* dan *request/respone.*
2. *Balanced transmission* merupakan mode komunikasi dimana setiap perangkat bisa bertindak sebagai pengendali dan pengontrol secara bersamaan, transmisi ini dibatasi untuk *point to point* dan *multi-point to point,* mode ini mendukung layanan seperti *send/confirm* dan *send/noreply.*

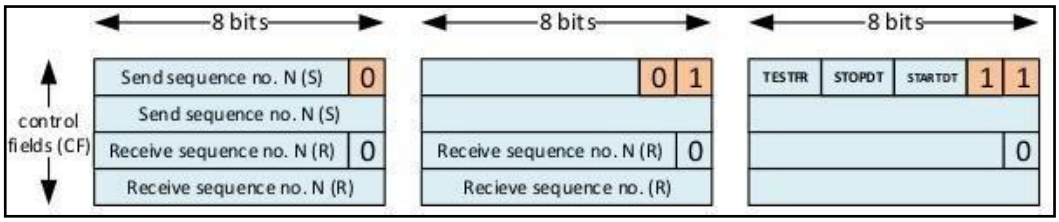
2.3.2. APCI Format

Pada APCI dimulai dengan bit awal bernilai 0x68, diikuti dengan panjang APDU 8 bit atau maksimal 253 byte dan empat *control fields* dengan panjang 4 byte, APDU bisa hanya terdiri dari APCI atau APCI dan ASDU.



Gambar 2.4 (a) Frame APDU dengan APCI dan (b) Frame APDU dengan APCI dan ASDU

Control Field terdiri dari 3 jenis format frame yaitu *I format*, *S format* dan *U format,* yang digunakan untuk melakukan transfer informasi *numbered, supervisory numbered* dan fungsi kontrol *unnumbered* (Maynard, 2014) . Frame format *control field* dapat dilihat pada Gambar 2.5 (a), (b) dan (c).

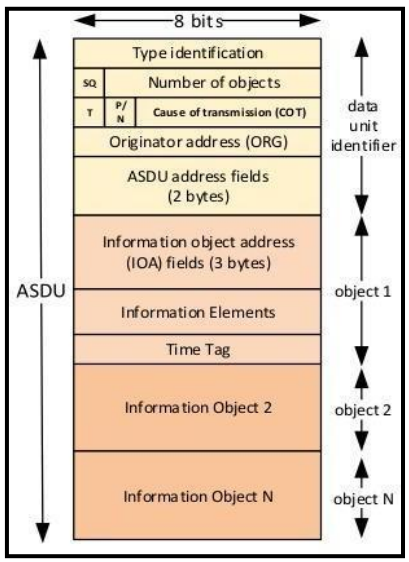


(a) (b) (c)

Gambar 2.5 (a) I Format, (b) S Format, (c) U Format

2.3.3. ASDU Format

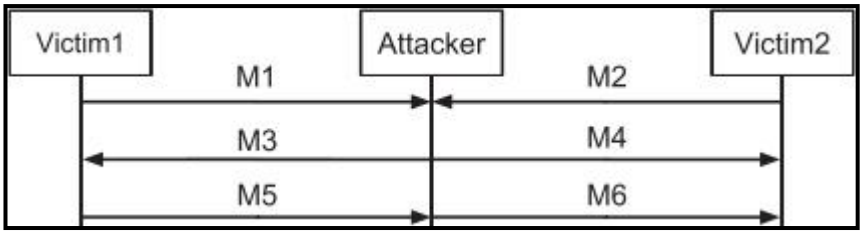
ASDU format terdiri dari dua bagian utama yaitu *data unit identifier* dengan panjang tetap 6 byte dan data itu sendiri terdiri dari satu atau lebih *object information.* D*ata unit identifier* mendefinisikan jenis data secara spesifik, memberikan pengalamatan untuk mengidentifikasi spesifik data dan termasuk informasi tambahan seperti *cause of transmission.* ASDU hanya dapat mengirimkan maksimal 127 objek. ASDU Format dapat dilihat pada gambar 2.6.



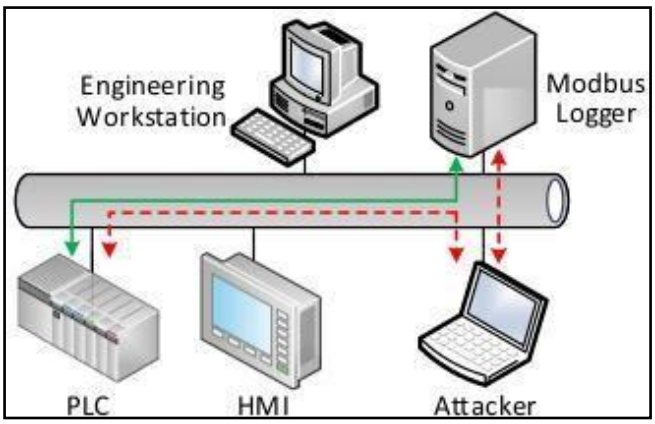
Gambar 2.6 ASDU Format

2.4. *Man In The Middle* (MITM)

Man In The Middle (MITM) adalah sebuah serangan dimana sebuah lalu lintas atau *traffic* jaringan antara dua host dicegat dan data dimonitor atau dimodifikasi dan diubah dalam sebuah komunikasi tanpa terdeteksi oleh korban. Tekni *ARP Spoofing / Poisoning* adalah teknik yang sering digunakan oleh penyerang dimana MITM dilakukan pada jaringan *Local Area Network* (LAN) (Celiktas, 2018). Serangan MITM dapat divisualisasikan seperti pada gambar 2.7 dan 2.8.



Gambar 2.7 Mode Skema Serangan MITM



Gambar 2.8 Mode Skema Serangan MITM pada SCADA

2.4.1. Tipe *Man In The Middle*

Menurut Conti (2016), serangan MITM terbagi menjadi beberapa bagian dan dapat dikategorikan menjadi 4 tipe dasar, yaitu :

1. *Spoofing*

Serangan MITM berdasarkan spoofing dimana penyerang melakukan interupsi terhadap trafik jaringan dan mengontrol data yang dikirimkan tanpa diketahui

oleh perangkat yang sedang berkomunikasi dengan cara meniru perangkat yang sah, ada empat jenis *spoofing* yaitu *ARP spoofing*, *DHCP spoofing*, *DNS spoofing* dan *IP spoofing.*

2. *SSL/TLS MITM*

Secure Socket Layer/Transport Layer Security adalah protocol enkripsi data untuk komunikasi pada internet, serangan MITM berdasarkan *SSL/TLS* dimana penyerang berada antara perangkat yang sedang berkomunikasi dan membuat dua koneksi SSL secara terpisah dan menyampaikan pesan di antara perangkat, dengan demikian penyerang bisa membaca semua pesan dan memodifikasi data.

3. *BGP MITM*

Border Gateway Protocol adalah mekanisme *routing* dengan memilih jalur tercepat dalam pengiriman data, BGP tidak memberikan autentikasi peer to peer, serangan MITM berdasarkan BGP dimana penyerang melakukan *IP hijacking* sehingga setiap pengiriman data akan melalui penyerang ini memungkinkan penyerang untuk melakukan modifikasi terhadap data yang dikirimkan.

4. FBS MITM

Serangan MITM berdasarkan *False Base Station* dimana penyerang membuat koneksi jaringan (misalnya Wi-Fi) palsu, koneksi jaringan ini bisa bertindak seperti koneksi asli dan memaksa korban untuk terhubung kemudian menggunakannya untuk memanipulasi trafik jaringan korban.

2.5. *TCP/IP* SCADA

Dalam sebuah serangan MITM yang terjadi pada jaringan SCADA agar serangan berhasil dilakukan adalah dengan penyerang harus berada dalam subnet yang sama dengan komputer target dan harus dapat meracuni (*poison)* cache *Address Resolution Protocol (ARP)* dari target atau korban (Chen, 2015).

Untuk melakukan serangan, *attacker* meracuni cache ARP dari router dan master Modbus. Ini dilakukan dengan menggunakan alat serangan MITM *source* yang disebut dengan Ettercap. Setelah penyerang mengetahui tentang server dan

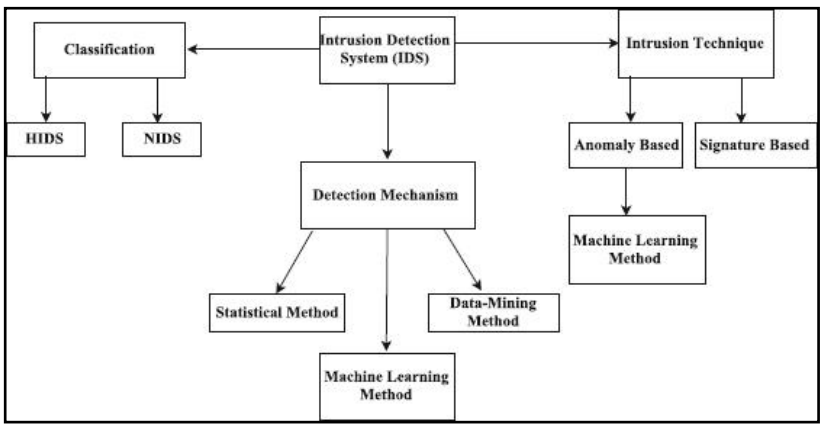
alamat IP korban, penyerang meniru klien Modbus dan dapat mengirim perintah Modbus untuk *Slave IED.*

Tabel 2.1 Komunikasi TCP/IP SCADA

MODBUS TCP/IP COMMUNICATION STACK			
#	**MODEL**	**IMPORTANT PROTOCOLS**	**REFERENCE**
7	Application	Modbus	
6	Presentation		
5	Session		
4	Transport	TCP	
3	Network	IP,ARP,RARP	
2	Data Link	Ethernet,CSMA/CD,MAC	IEEE 802.3
1	Physical	Ethernet Physical Layer	Ethernet

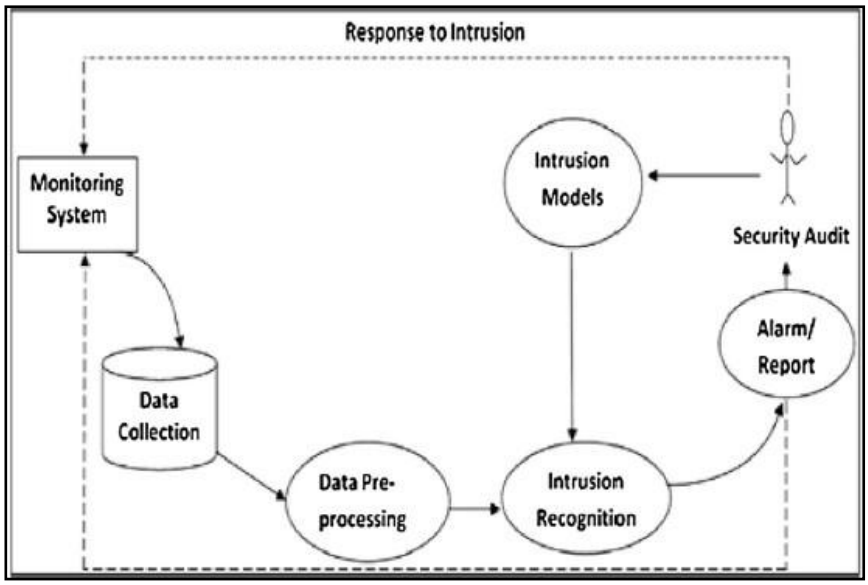
2.6. *Intrusion Detection System*

Intrusion Detection System (IDS) adalah sebuah aplikasi *software* atau perangkat keras yang digunakan untuk mendeteksi sebuah serangan dengan menganalisa pola lalu lintas data dalam jaringan (Kunang, 2019). IDS dapat diimplementasikan menggunakan metode dan teknik yang berbeda, gambar 2.9 menunjukkan metode dan teknik yang digunakan dalam IDS, yaitu :



Gambar 2.9 Metode dan Teknik IDS

IDS dipasang pada jaringan sebagai sensor untuk mendeteksi setiap trafik jaringan yang dicurigai sebagai aktivitas berbahaya. Gambar 2.10 menunjukkan struktur dari IDS, yaitu:



Gambar 2.10 Struktur IDS

2.7. Klasifikasi IDS Berdasarkan Penempatan *Deployment*

Klasifikasi *Intrusion Detection System* ini mengacu pada penempatan *Deployment* infrastruktur system, dibagi menjadi dua yaitu *Host-based Intrusion Detection System* (HIDS) dan *Network-based Intrusion Detection System* (NIDS) (Aljawarneh, 2018). *Host-based Intrusion Detection System* adalah IDS yang ditempatkan pada perangkat *host,* digunakan untuk monitoring dan menganalisa proses yang terkait dengan file aplikasi system dan system operasi. Sedangkan, *Network-based Intrusion Detection System* adalah IDS yang ditempatkan pada jaringan, digunakan untuk menangkap dan menganalisa trafik jaringan.

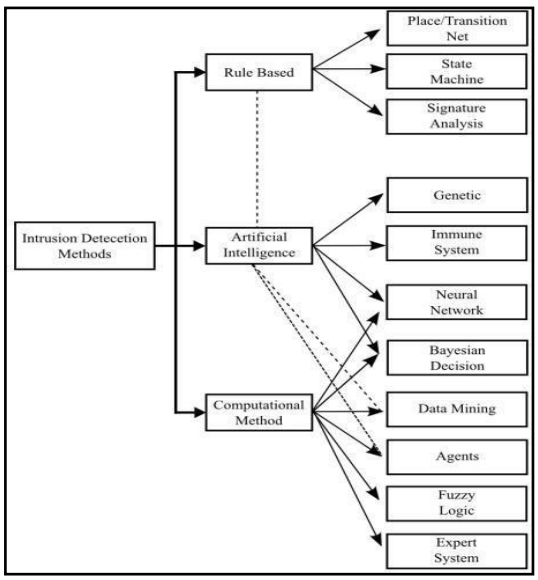
2.8. Klasifikasi IDS Berdasarkan Metode Deteksi

Klasifikasi *Intrusion Detection System* berdasarkan metode deteksi mengacu pada bagaimana IDS menganalisa trafik data yang melalui jaringan maupun *host,* dibagi dua yaitu *anomali-based system* dan *signature-based system*

(Chaabouni, 2019). *Anomali-based system* memodelkan perilaku system normal dan membandingkan dengan perilaku yang dipantau untuk model dasar, jika perilaku tertentu berbeda dengan perilaku normal, maka IDS akan mengklasifikasikan tindakan tersebut sebagai serangan, teknik ini mampu mendeteksi serangan yang tidak diketahui, namun mempunyai kelemahan dengan *false positif alert.* Sedangkan, *signature-based system* memodelkan perilaku serangan dan menyimpannya ke basis data *signature* serangan, dalam deteksi IDS membandingkan *signature* serangan dengan trafik jaringan, teknik ini tidak dapat mendeteksi serangan yang tidak terdapat pada basis data *signature* serangan.

2.9. Metode Penelitian Umum IDS

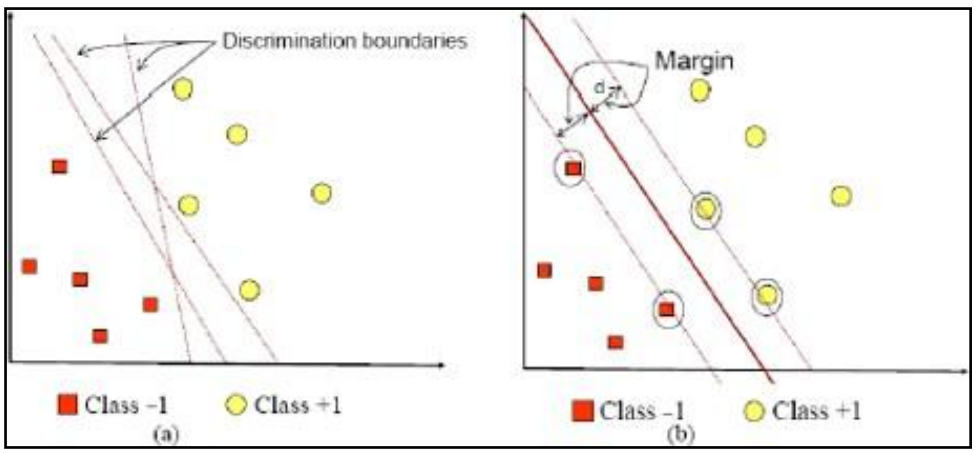
Metode penelitian umum pada perancangan *Intrusion Detection System* dibagi menjadi tiga bagian yaitu *Rule Based, Artificial Intelligence* dan *Computational Method.* Pada metode *Rule Based* terdiri dari empat bagian di antaranya *State Machine, Place Net* dan *Signature Analysis*. Sedangkan pada metode *Artificial Intelligence* dibagi menjadi empat bagian yaitu *Neural Network, Genetic, Immune System* dan *Bayesian Decision.* Serta pada metode *Computational Method* dibagi menjadi beberapa bagian yaitu *Data Mining, Neural Network, Bayesian Decision, Agents, Fuzzy Logic* dan *Expert System* (Akbar, 2019).



Gambar 2.11 Diagram Metode Penelitian Umum IDS

2.10. *Support Vector Machine*

Support Vector Machine (SVM) adalah bagian *machine learning* yang bekerja atas prinsip Structural Risk *Minimization* (SRM) yaitu mencari nilai resiko terkecil dalam menentukan vektor tertentu menjadi bagian dari sebuah kelas dengan tujuan menemukan hyperplane terbaik yang memisahkan dua class. SVM menciptakan *hyperplane* atau *multiplane* dalam ruang berdimensi yang tinggi. SVM juga merupakan teknik pembelajaran yang diawasi dan dilatih untuk mengklasifikasi berbagai kategori datanya (Kurnaz, 2018). Dalam SVM memiliki dua klasifikasi yaitu data linier dan *non linear*, dimana klasifikasi *non linier* ini menggunakan fungsi kernel untuk memperkirakan format margin yang telah banyak digunakan dalam aplikasi pemrosesan gambar dan pengenalan pola.



Gambar 2.12 Support Vector Machine

2.11. Evaluasi Performa Metode *Support Vector Machine*

Pada evaluasi system klasifikasi *biner* yang dihitung menggunakan *confusion matrix* (Deng, 2016). Untuk melakukan evaluasi diperlukan perhitungan akurasi yang berdasarkan statistika dengan parameter pada *confusion matrix.* Nilai yang didapatkan pada *confusion matrix* dapat berbeda – beda tergantung pada jumlah data latih dan uji yang didapatkan. Adapun jenis performa yang dapat kita hitung menggunakan *confusion matrix* yaitu :

Parameter Confusion Matrix

	labelled positive	labelled negative
predicted positive	*TP*	*FP*
predicted negative	*FN*	*TN*

Gambar 2.13 Confusion Matrix

Keterangan:

1. *True Positive* (TP)

   Pada true positive menunjukkan sejumlah data normal yang diklasifikasi dengan benar sebagai data normal yang didapatkan.

2. *False Positive* (FP)

   Pada *false positive* yang menunjukkan sejumlah data serangan yang diklasifikasi sebagai data normal yang didapatkan.

3. *True Negative* (TN)

   Pada *true negative* menunjukkan jumlah data serangan yang diklasifikasi dengan benar sebagai data serangan yang didapatkan.

4. *False Negative* (FN)

   Pada *false negative* yang menunjukkan sejumlah data serangan yang diklasifikasi sebagai data normal yang didapatkan.

Pada umumnya untuk mengukur performa dari hasil klasifikasi *Intrusion Detection System* hal yang dievaluasi adalah *accuracy*, *detection rate, false alert rate* dan *precision.* Dengan model matematis seperti pada gambar 2.14.

$$Accuracy = \frac{TP+TN}{TP+TN+FP+FN}$$

$$TPR = \frac{TP}{TP+FN}$$

$$FPR = \frac{FP}{TN+FP}$$

$$TNR = \frac{TN}{TN+FP}$$

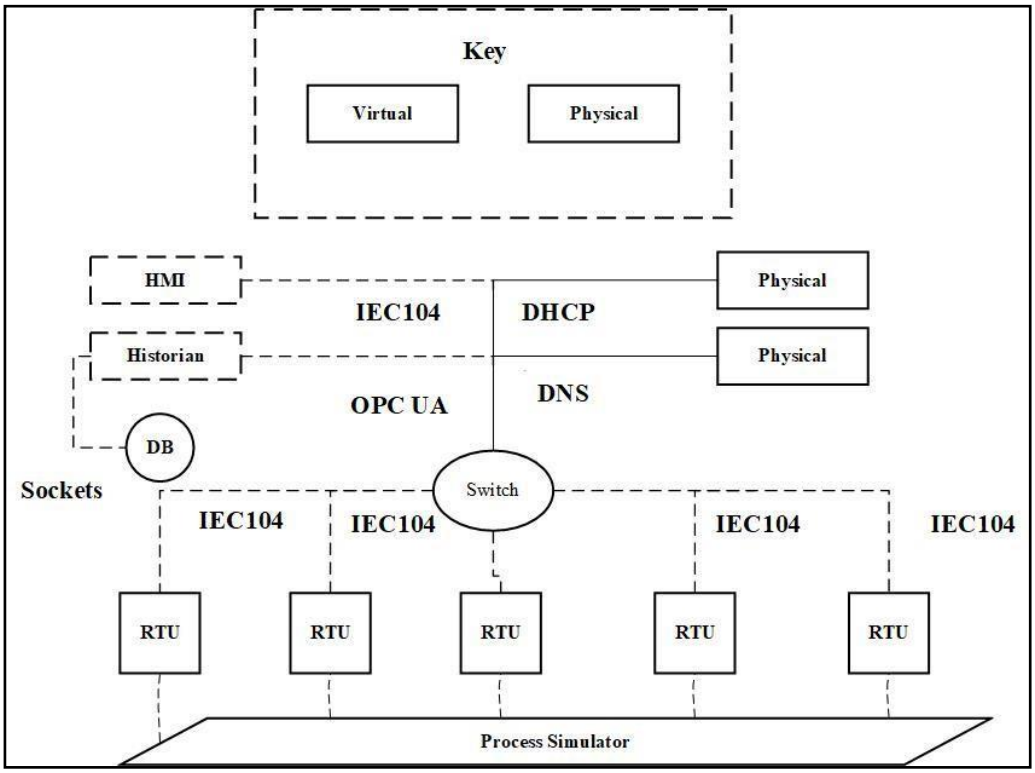
$$FNR = \frac{FN}{FN+TP}$$

$$Precision = \frac{TP}{TP+FP}$$

Gambar 2.14 Rumus Matematis Performa

2.12. Dataset

Dataset pada penelitian ini merupakan dataset yang dikembangkan oleh penelitian Maynard (2018) yang berisi trafik data normal dan serangan dalam simulasi lingkungan *testbed.* Dataset dibangun menggunakan sejumlah mesin virtual yang mereplikasi jaringan *Supervisory Control And Data Acquisition,* termasuk beberapa *host virtual* untuk sensor dan aktuator. Evaluasi dataset ini dilakukan pada tahun 2018 disediakan dalam bentuk format *pcap.* Gambar 2.15 memperlihatkan diagram jaringan sampel *testbed* dataset ini.



Gambar 2.15 Diagram *Network sample Testbed*

Dataset dibangun dengan melakukan serangan *Man In The Middle* pada protocol IEC 104 yang menyebabkan nilai *valid* dari *Cause of Transmission* (CoT) menjadi nilai *invalid.*