SISTEM DETEKSI *MAN IN THE MIDDLE* (MITM) ATTACK PADA JARINGAN *SUPERVISORY CONTROL AND DATA ACQUISITION* (SCADA) DENGAN MENGGUNAKAN *DECISION TREE*

TUGAS AKHIR

Oleh :

M. Rozzak Farhan
09011181621014

JURUSAN SISTEM KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS SRIWIJAYA

2021

SISTEM DETEKSI *MAN IN THE MIDDLE* (MITM) ATTACK PADA JARINGAN *SUPERVISORY CONTROL AND DATA ACQUISITION* (SCADA) DENGAN MENGGUNAKAN *DECISION TREE*

TUGAS AKHIR

Diajukan Untuk Melengkapi Salah Satu Syarat
Memperoleh Gelar Sarjana Komputer

Oleh :

M. Rozzak Farhan
09011181621014

JURUSAN SISTEM KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS SRIWIJAYA
2021

LEMBAR PENGESAHAN

SISTEM DETEKSI *MAN IN THE MIDDLE* (MITM) ATTACK PADA JARINGAN *SUPERVISORY CONTROL AND DATA ACQUISITION* (SCADA) DENGAN MENGGUNAKAN *DECISION TREE*

TUGAS AKHIR

Diajukan Untuk Melengkapi Salah Satu Syarat
Memperoleh Gelar Sarjana Komputer

Oleh :

M. Rozzak Farhan
09011181621014

Indralaya, Desember 2021

Mengetahui,

Pembimbing Tugas Akhir I	Pembimbing Tugas Akhir II
Deris Stiawan, M.T., Ph.D	**Ahmad Heryanto, S.Kom., M.T.**
NIP. 197806172006041002	**NIP. 198701222015041002**

Ketua Jurusan Sistem Komputer 20/1/22

Dr. Ir. Sukemi, M.T.
NIP. 196612032006041001

HALAMAN PERSETUJUAN

Telah diuji dan lulus pada :

Hari : Kamis
Tanggal : 2 Desember 2021

Tim Penguji :

1. **Ketua** : **Sarmayanta Sembiring, S.SI., M.T.**
2. **Sekretaris** : **Huda Ubaya, S.T., M.T.**
3. **Pembimbing I** : **Deris Stiawan, M.T., Ph.D.**
4. **Pembimbing II** : **Ahmad Heryanto,S.Kom., M.T**

Mengetahui,
Ketua Jurusan Sistem Komputer

Dr. Ir. Sukemi, M.T
NIP. 196612032006041001

LEMBAR PERNYATAAN

Yang bertanda tangan dibawah ini:

Nama : M. Rozzak Farhan

NIM : 09011181621014

Judul : Sistem Deteksi *Man In The Middle* (MITM) Attack Pada Jaringan *Supervisory Control And Data Acquisition* (SCADA) dengan Menggunakan *Decision Tree*

Hasil Pengecekan *Software iThenticate/Turnitin* : 14%

Menyatakan bahwa laporan tugas akhir saya merupakan hasil karya sendiri dan bukan hasil penjiplakan / plagiat dari penelitian orang lain. Apabila ditemukan unsur penjiplakan / plagiat dalam laporan tugas akhir ini, maka saya bersedia menerima sanksi akademik dari Universitas Sriwijaya sesuai dengan ketentuan yang berlaku.

Demikian pernyataan ini saya buat dalam keadaan sadar dan tidak dipaksakan.

Indralaya, Desember 2021

M. Rozzak Farhan
09011181621014

HALAMAN PERSEMBAHAN

"Maka sesungguhnya bersama kesulitan ada kemudahan" -

(Q.S. Al-Inshirah : 6)

"Everything is finally okay"

Segenap hati berterima kasih dengan penuh rasa sayang kepada :

- *Ibu (Ningsih, S.Pd.) dan Bapak (Parianto) tercinta*
- *Kakak (Jia Hatimah S.Kom) tersayang*
- *Keluarga dan saudara yang memberikan dukungan*
- *Dosen Pembimbing Tugas Akhir 1: Deris Stiawan, M.T, Ph.d. dan Pembimbing Tugas Akhir 2: Ahmad Heryanto, S.kom, M.T.*
- *Dosen Pembimbing Akademik Prof. Dr. Ir. Siti Nurmaini, M.T.*
- *Teman-teman seperjuangan SK 2016 dan Himasisko*
- *Keluarga Besar Sistem Komputer Universitas Sriwijaya*
- *Civitas Akademika Universitas Sriwijaya*
- *Kepada diri saya Sendiri*

KATA PENGANTAR

Puji syukur atas kehadirat Allah SWT, atas segala karunia dan rahmat-Nya sehingga penulis dapat menyelesaikan penulisan Proposal Tugas Akhir ini dengan judul **"Sistem Deteksi *Man In The Middle* (MITM) *Attack* Pada Jaringan *Supervisory Control And Data Acquisition* (SCADA) Dengan Menggunakan *Decision Tree*".**Penulisan Proposal Tugas Akhir ini dilakukan untuk melengkapi salah satu syarat memperoleh gelar Sarjana Komputer di Jurusan Sistem Komputer Fakultas Ilmu Komputer Universitas Sriwijaya. Adapun sebagai bahan penulisan, penulis mengambil berdasarkan hasil penelitian, observasi dan beberapa sumber literatur yang mendukung dalam penulisan proposal ini. Pada kesempatan ini juga, penulis menyampaikan ucapan terima kasih yang sebesar-besarnya kepada semua pihak yang telah membantu baik dari segi moril ataupun materil serta memberikan kemudahan, dorongan, saran dan kritik selama dalam proses penulisan Proposal Tugas Akhir ini.

Oleh karena itu, pada kesempatan ini penulis mengucapkan rasa syukur kepada Allah SWT. dan mengucapkan terima kasih kepada yang terhormat :

1. Orang Tua serta keluarga penulis tercinta, yang telah memberikan doa dan restu serta dukungan yang sangat besar selama mengikuti dan melaksanakan perkuliahan di Jurusan Sistem Komputer Fakultas Ilmu Komputer Universitas Sriwijaya hingga dapat menyelesaikan Proposal Tugas Akhir ini.
2. Bapak Jaidan Jauhari, S.Pd., M.T., selaku Dekan Fakultas Ilmu Komputer Universitas Sriwijaya.
3. Bapak Dr. Ir. Sukemi, M.T.**,** selaku Ketua Jurusan Sistem Komputer Fakultas Ilmu Komputer Universitas Sriwijaya.
4. Bapak Prof. Dr. Ir. Siti Nurmaini, M.T. selaku Dosen Pembimbing Akademik di Jurusan Sistem Komputer Fakultas Ilmu Komputer Universitas Sriwijaya.
5. Bapak Deris Stiawan, M.T., Ph. D, selaku Dosen Pembimbing Tugas Akhir di Jurusan Sistem Komputer Fakultas Ilmu Komputer Universitas Sriwijaya.
6. Bapak Ahmad Heryanto, S.Kom,. M.T. selaku Dosen Pembimbing II Tugas Akhir di Jurusan Sistem Komputer Fakultas Ilmu Komputer Universitas Sriwijaya.

7. Mbak Reny selaku admin Jurusan Sistem Komputer yang telah membantu mengurus seluruh berkas.
8. Seluruh dosen, staff, serta karyawan Fakultas Ilmu Komputer Universitas Sriwijaya.
9. Seluruh teman-teman seperjuangan semuanya yang saling membantu dalam hal apapun.

Akhir kata penulis menyadari bahwa dalam penulisan Proposal Tugas Akhir ini masih jauh dari kesempurnaan. Oleh karena itu, penulis memohon saran dan kritik yang sifatnya membangun demi kesempurnaan Tugas Akhir ini dan semoga bermanfaat bagi kita semua baik dalam dunia Pendidikan maupun dalam lingkungan masyarakat. Aamiin.

Indralaya, Desember 2021

Penulis

M. Rozzak Farhan

NIM. 09011181621014

Man In The Middle (MITM) Attack Detection System on Supervisory Control And Data Acquisition (SCADA) Networks Using Decision Trees

M. Rozzak Farhan (09011181621014)
Departement of Computer Engineering, Faculty of Computer Science,
Sriwijaya University
Email: mrozzakfarhan@gmail.com

Abstract

Supervisory Control and Data Acquisition (SCADA) is a control system that allows monitoring and management of industrial processes remotely and controlled by using a computer network. In the SCADA system, there are several protocols, one of the communication protocols is IEC 60870-5-104 or also known as IEC-104. Man In The Middle (MITM) attack is one of the most common types of security attacks, which illustrates that MITM attacks are also a security threat on SCADA networks. One of the MITM attacks is ARP Spoofing which can perform network scans. Intrusion Detection System (IDS) is a system to detect traffic in a network. The IDS will provide a warning when it detects an attack. A decision tree is an algorithm method used for classification techniques that have the aim of making predictions on the data. The best performance results produced by Decision Tree are with an accuracy rate of 97.52%.

Keywords: *Supervisory Control and Data Acquisition* (SCADA), *Man In The Middle* (MITM), *Decision Tree*

Sistem Deteksi *Man In The Middle* (MITM) Attack Pada Jaringan *Supervisory Control And Data Acquisition* (SCADA) dengan Menggunakan *Decision Tree*

M. Rozzak Farhan (09011181621014)
Jurusan Sistem Komputer, Fakultas Ilmu Komputer,
Universitas Sriwijaya
Email: mrozzakfarhan@gmail.com

Abstrak

Supervisory Control and Data Acquisition (SCADA) adalah suatu sistem kontrol yang memungkinkan pemantauan dan pengelolaan proses industri dari jarak jauh dan dikendalikan dengan memanfaatkan jaringan komputer. Pada sistem SCADA terdapat beberapa protokol, salah satu protokol komunikasi tersebut adalah IEC 60870-5-104 atau dikenal juga dengan IEC-104. Serangan *Man In The Middle* (MITM) merupakan salah satu jenis serangan keamanan yang paling umum, yang menggambarkan serangan MITM juga merupakan ancaman keamanan pada jaringan SCADA. Salah satu serangan MITM adalah *ARP Spoofing* yang bisa melakukan *network scanning. Intrusion Detection System* (IDS) merupakan suatu sistem untuk mendeteksi lalu lintas dalam sebuah jaringan. IDS akan memberikan *alert* ketika mendeteksi serangan. *Decision tree* adalah suatu metode algoritma yang digunakan untuk teknik klasifikasi yang mana mempunyai tujuan untuk melakukan prediksi terhadap sekumpulan data. Hasil performa terbaik yang dihasilkan oleh *Decision Tree* ialah dengan tingkat akurasi sebesar 97.52%.

Kata Kunci: *Supervisory Control and Data Acquisition* (SCADA), *Man In The Middle* (MITM), *Decision Tree*

DAFTAR ISI

Halaman

DAFTAR GAMBAR

Halaman

DAFTAR TABEL

Halaman

DAFTAR RUMUS

Halaman

BAB I
PENDAHULUAN

1.1 Latar Belakang

Supervisory Control and Data Acquisition (SCADA) adalah suatu sistem kontrol yang memungkinkan pemantauan dan pengelolaan proses industri dari jarak jauh dan dikendalikan dengan memanfaatkan jaringan komputer [1]. *Supervisory Control And Data Acquisition* (SCADA) adalah *Industry Control System* (ICS) automatis yang digunakan untuk monitoring dan kendali proses di *sector industry* dan infrastuktur nasional [2]. *Sistem Supervisory Control and Data Acquisition* (SCADA) sekarang telah diintegrasikan ke dalam infrastruktur penting seperti pembangkit tenaga listrik, sistem transportasi, distribusi air, dan sistem pengumpulan air limbah untuk mengontrol dan memantau proses industri tersebut [3]. Namun, saat ini, sistem ini terhubung ke Internet untuk menyediakan kemampuan kendali jarak jauh, yang membuatnya rentan terhadap pihak lawan, yang bertujuan untuk mengganggu proses yang dikendalikan.

Pada sistem SCADA terdapat beberapa protokol, salah satu protokol komunikasi tersebut adalah IEC 60870-5-104 atau dikenal juga dengan IEC-104 yang mana digunakan untuk mengirimkan pesan untuk telekontrol dasar antar perangkat berdasarkan TCP/IP, yang memungkinkan transmisi data secara simultan antara beberapa perangkat dan layanan [4]. IEC-104 adalah protokol yang merupakan gabungan dari *application message* dari protokol IEC-101 dengan protokol TCP/IP.

Serangan *Man-In-The-Middle* (MITM) adalah salah satu serangan paling terkenal dalam keamanan komputer, mewakili salah satu masalah terbesar bagi para profesional keamanan. MITM menargetkan data aktual yang mengalir diantara titik akhir, dan kerahasiaan serta integritas data itu sendiri [5]. Nama *Man-In-The-Middle* berasal dari skenario bola basket dimana dua pemain bermaksud untuk mengoper bola satu sama lain, sedangkan salah satu pemain diantara keduanya mencoba untuk merebutnya. Serangan MITM juga dikenal sebagai: Serangan *Monkey-in-the-middle*, *Session hijacking*, TCP *hijacking*, TCP *session hijacking* [5].

Serangan MITM dapat dibagi menjadi empat tipe dasar. Pertama, serangan MITM berbasis *Spoofing* dimana musuh mencegat lalu lintas yang sah dengan bantuan serangan *spoofing* dan mengontrol data. Kedua, serangan MITM SSL/TSL dimana musuh memasukkan dirinya sendiri ke dalam saluran komunikasi antara dua titik akhir atau korban. Ketiga, serangan BGP MITM dimana musuh mengirimkan lalu lintas yang dicuri ke tujuan. Terakhir, serangan *MITM base station* palsu dimana musuh membuat stasiun transceiver palsu dan kemudian menggunakannya untuk memanipulasi lalu lintas korban.

Serangan MITM merupakan salah satu jenis serangan keamanan yang paling umum, yang menggambarkan serangan MITM juga merupakan ancaman keamanan pada jaringan SCADA. Maka dari itu dibutuhkan metode untuk membantu mendeteksi serangan MITM dalam SCADA. Dengan menggunakan perhitungan statistika dan algoritma yang matematis *Machine Learning* dapat digunakan untuk mengetahui informasi yang tersembunyi ataupun data yang mencurigakan [6]. *Machine Learning* merupakan studi ilmiah tentang algoritma dan model statistik yang digunakan sistem komputer untuk melakukan suatu tugas tertentu. Algoritma pembelajaran mesin membangun model matematika berdasarkan data sampel,yang dikenal sebagai '*Data Training*' untuk membuat prediksi atau suatu keputusan.. Pada percobaan [7] ada beberapa algoritma *Machine Learning* untuk mengenali serangan pola serangan salah satunya adalah *Decision Tree.* Berdasarkan pembahasan di atas maka penelitian ini mendeteksi serangan *Man In The Middle* (MITM) pada jaringan *Supervisory Control and Data Acquisition* (SCADA) *de*ngan menggunakan *Decision Tree*.

1.2 Tujuan

Adapun tujuan dari penulisan Tugas Akhir ini adalah sebagai berikut:

1. Mendeteksi serangan MITM pada jaringan SCADA dengan metode *Decision Tree*.
2. Mengetahui pola serangan MITM pada jaringan SCADA.
3. Melakukan klasifikasi dengan menggunakan metode *Decision Tree*.
4. Mendapatkan akurasi dari serangan MITM dengan metode *Decision Tree.*

1.3 Manfaat

Adapun manfaat dari penulisan Tugas Akhir ini adalah sebagai berikut:

1. Dapat mendeteksi *Man In The Middle Attack* pada jaringan SCADA dengan metode *Decision Tree*
2. Dapat mengetahui pola serangan pada dataset.
3. Dapat mendeteksi *Man In The Middle Attack* pada jaringan SCADA dengan metode *Decision Tree*
4. Memberikan informasi mengenai keakurasian metode *Decision Tree* dalam deteksi pola lalu lintas jaringan SCADA yang terjadi *Man In The Middle Attack.*

1.4 Rumusan Masalah

Berikut adalah rumusan masalah dalam penulisan Tugas Akhir ini:

1. Bagaimana cara mengekstrak dataset ?
2. Apakah *snort engine* dapat mendeteksi serangan pada dataset?
3. Bagaimana cara mengetahui pola serangan MITM dari dataset? Bagaimana cara mengali pola serangan MITM?

1.5 Batasan Masalah

Batasan masalah Tugas Akhir ini yaitu sebagai berikut:

1. Dalam penelitian ini serangan yang digunakan adalah MITM.
2. Metode yang digunakan untuk mendeteksi serangan adalah *Decision Tree.*
3. Menggunakan dataset online dari Situs Figshare.
4. Hanya mengenali dan mendeteksi serangan di protokol IEC104.
5. Bersifat *Offline*.
6. Tidak membahas cara pencegahan serangan *Man in The Middle*.

1.6 Metodologi Penelitian

Metodologi yang digunakan dalam penulisan Tugas Akhir ini akan melewati beberapa tahapan sebagai berikut:

1. Studi pustaka

Pada tahapan ini penulis mengkaji dan memahami referensi dari media pembelajaran dengan membaca buku, naskah ilmiah, serta artikel yang terkait langsung dengan penelitian ini.

2. Perancangan Sistem

Pada tahapan ini penulis merancang dan membuat sistem deteksi serangan *Man in The Middle* menggunakan algoritma *Decision Tree* dan menentukan perangkat-perangkat yang diperlukan pada penelitian ini, baik perangkat keras maupun perangkat lunak.

3. Pengujian

Pada tahapan ini penulis melakukan pengujian sesuai dengan batasan masalah pada penelitian ini.

4. Hasil dan Analisis

Pada tahapan ini penulis melakukan analisis terhadap hasil pengujian tersebut untuk mengetahui apa kelebihan dan kekurangan rancangan sistem serta faktor yang mempengaruhi.

5. Kesimpulan dan Saran

Pada tahapan ini penulis mengambil kesimpulan berdasarkan rumusan masalah, studi pustaka, metodologi dan analisis hasil pengujian, serta memberikan saran untuk penelitian selanjutnya

1.7 Sistematika Penulisan

Adapun sistematika penulisan dalam Proposal Tugas Akhir ini adalah sebagai berikut:

BAB I. PENDAHULUAN

Bab I akan berisikan latar belakang masalah, tujuan dan manfaat serta metodologi penelitian dan sistematika penulisan.

BAB II. TINJAUAN PUSTAKA

Bab II akan berisi dasar teori jaringan *Supervisory Data and Acquisition (SCADA)*, *Man In The Middle* (MITM)*, Machine Learning*, dan metode *Decision Tree*.

BAB III. METODOLOGI PENELITIAN

Bab III akan membahas deteksi dan analisis serangan *Man In The Middle* di jarigan SCADA dengan menggunakan metode *Decision Tree*

BAB IV. IMPLEMENTASI PENGUJIAN

Bab IV membahas proses implementasi perangkat lunak dari hasil deteksi *Man In The Middle* (MITM) *Attack* dengan menggunakan metode *Decision Tree*.

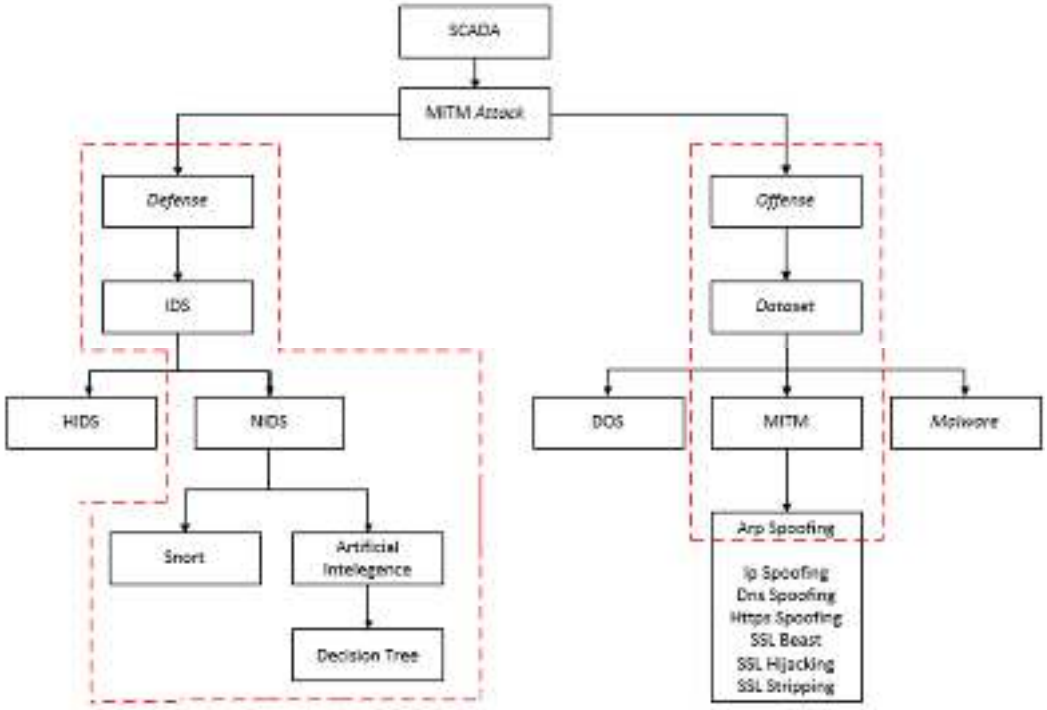
BAB V. KESIMPULAN DAN SARAN

Bab V berisi kesimpulan dari bab-bab yang sudah dicantumkan mengenai hasil dari pengimplementasian metode *Decision Tree* dalam mendeteksi *Man In The Middle* (MITM) *Attack.* Pada bab ini juga akan berisi saran yang diharapkan dapat digunakan untuk penelitian selanjutnya.

BAB II
TINJAUAN PUSTAKA

2.1 Diagram Konsep Penelitian

Pada penelitian tugas akhir ini mempunyai beberapa bagian atau sub materi yang akan dibahas, oleh sebab itu perlu dirancang sebuah kerangka konsep secara berurutan untuk menampilkan pembahasan penelitian secara keseluruhan, seperti yang bisa dilihat pada gambar dibawah ini:

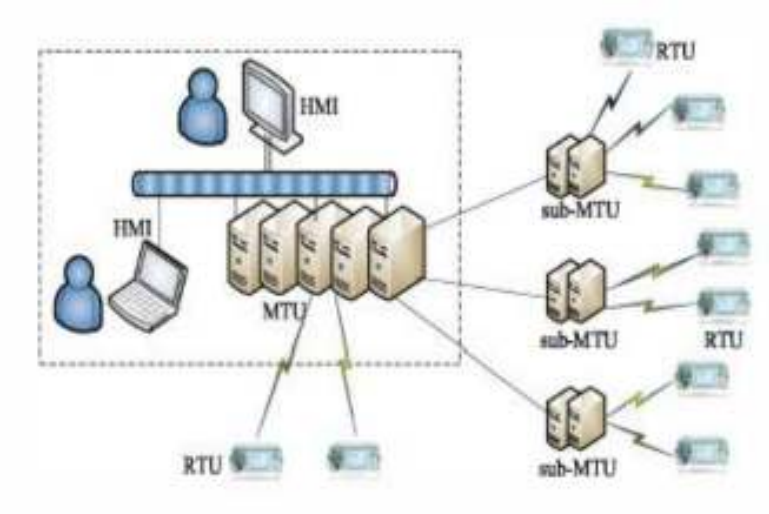


Gambar 2.1 Diagram Konsep Penelitian

2.2 *Supervisory Control And Data Acquisition* (SCADA)

Supervisory Control and Data Acquisition (SCADA) adalah sistem yang termasuuk dalam *Industrial Control Systems* (ICS) yang banyak digunakan oleh industri untuk memantau dan mengontrol berbagai proses seperti jaringan pipa minyak dan gas, distribusi air, jaringan tenaga listrik, dll. [8]. Sistem ini menyediakan kontrol otomatis dan pemantauan jarak jauh dari layanan yang digunakan dalam kehidupan sehari-hari. Sistem 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 sistem SCADA sangat penting dalam proses industri

karena membutuhkan akuisisi dan kontrol data secara *realtime* [2]. Operasi sistem SCADA sepenuhnya bergantung pada data yang diterima dari RTU, yang menjadi dasar pengendalian tindakan yang akan diambil [9].

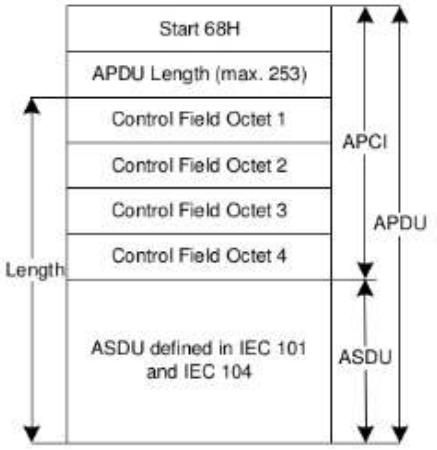


Gambar 2.2 SCADA Arsitektur [10].

HMI adalah subsistem dari SCADA yang berfungsi menampilkan data dari hasil pengukuran di RTU ataupun menampilkan proses yang sedang terjadi pada keseluruhan sistem. MTU atau *Master Terminal Unit* merupakan sebuah sistem komputer (bisa komputer bisa PLC atau bahkan *microcontroller*) yang bertugas memberikan data kepada HMI dari RTU. RTU atau *Remote Terminal Unit* adalah subsistem SCADA yang berfungsi sebagai terminal-terminal dari hasil pengukuran, pengendalian, pemantauan status dan lain-lain.

2.3 Protocol IEC-60870-5-104 / IEC-104

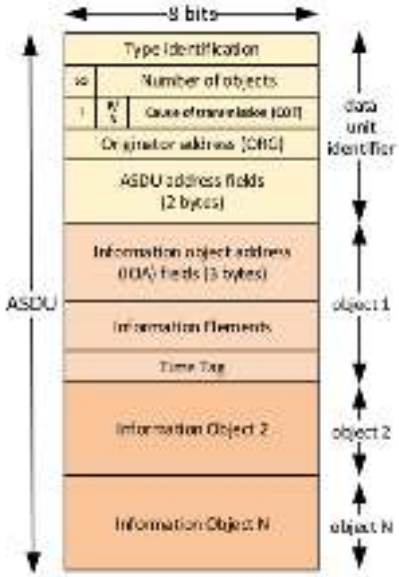
Ada banyak standar komunikasi internasional yang digunakan untuk pengoperasian sistem SCADA. Yang paling terkenal adalah Modbus, Distributed Network Protocol (DNP3), Profinet, IEC-60870-5 dan IEC-61850 [11]. IEC 60870 adalah standar untuk interoperabilitas diantara item telekontrol yang kompatibel. Spesifikasi standar untuk protokol IEC 60870-5-104 adalah kombinasi dari lapisan aplikasi IEC 60870-5-101 dan protokol TCP / IP. IEC 60870-5-101[7]. Setiap paket *payload* IEC-104 disebut *Application Protocol Data Unit* (APDU) [12]. APDU dibagi jadi 2 menjadi dua bagian: *Application Service Data Unit* (ASDU) *dan Application Protocol Control Information* (APCI).



Gambar 2.3 *Payload* Paket IEC 60870- 5-104 / APDU [13].

2.3.1 *Application Service Data Unit* (ASDU)

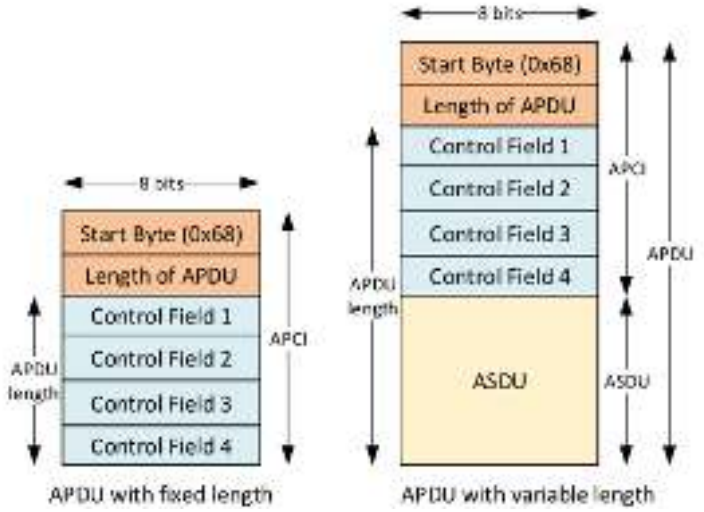
ASDU menentukan jenis fungsi (yang disebut ID jenis) yang mereka bawa. Mereka dapat berisi hingga 127 Objek Informasi (IO), mengacu pada alamat berbeda di RTU yang sedang dikontrol [12]. ASDU berisi dua bagian utama: pengenal unit data (engan Panjang teteap enam *byte*), dan data itu sendiri, terdiri dari satu atau lebih objek informasi [14]. Pengidentifikasi unit data mendefinisikan tipe data tertentu, memberikan pengalamatan untuk mengidfentifikasi identitas spesifik dari data, dan memasukkan informasi tambahan sebagai penyebab transmisi.



Gambar 2.4 ASDU Format

2.3.2 *Application Protocol Control Information* (APCI)

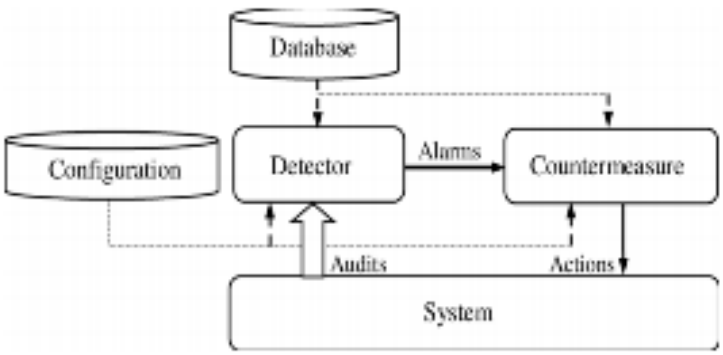
APCI digunakan sebagai mekanisme komunikasi *start* dan *stop* untuk ASDU. APCI berisi karakter awal, 68H *length field* (berisi panjang APDU) dan *control field*. Setiap APCI yang dimulai dengan *byte* awal dengan nilai 0x68 diikuti oleh APDU 8-bit dan 4 8-bit *control fields.* APDU bisa berisi APCI atau APCI dan ASDU.



Gambar 2.5 APCI Format

2.4 *Intrusion Detection System* (IDS)

Intrusion Detection System (IDS) merupakan *alarm* intrusi dalam keamanan jaringan. Dimana tidak memberi respon terhadap paket serangan yang terdeteksi tetapi hanya memberikan *alert* [15]. IDS merupakan kombinasi dari *hardware* dan *software* yang memiliki fungsi untuk melakukan monitoring sistem atau jaringan dari aktifitas malicious yang dilakukan oleh attacker.



Gambar 2.6 Arsitektur Dasar IDS [16]

2.5 Klasifikasi IDS

2.5.1 Klasifikasi IDS Sumber Data (*Data Resource*)

a. NIDS (*Network-based Intrusion Detection System*)

Metode NIDS ini melakukan analisis terhadap paket dala yang berjalan melalui lalu lintas jaringan yang akan ke alamat *host*. Data yang ditangkap pada lalu lintas jaringan ini selanjutnya di-*capture* yang selanjutnya di lakukan pencocokan terhadap *signature* yang telah ada pada *database*.

b. HIDS (*Host-based Intrusion Detection System*)

Metode ini digunakan pada pihak *host* yang dimulai dari log sistem, operasi sistem dan pada program aplikasi. Dengan tujuan dapat mendeteksi dari sebuah intrusi pada sistem tersebut. Sistem IDS dengan metode HIDS ini terdapat dua kategori yaitu sistem yang meberikan *alert* pada *host* jika terdapat intrusi, dan ada yang bersifat *real time* secara *default*.

c. *Hybrid* IDS

Sistem *hybrid* menggunakan pengetahuan parsial dari keduanya, yaitu, informasi normal dan serangan untuk mendeteksi serangan. Dengan demikian, mereka memiliki kinerja yang lebih baik, menghasilkan lebih sedikit *false alarm* dan meningkatkan tingkat deteksi serangan.

2.5.2 Klasifikasi IDS Metode Deteksi IDS

a. *Signature Based*

Signature–Based merupakan proses deteksi yang dilakukan dengan cara mencocokkan data pada database yang telah teserdia. Dengan kekurangan tidak dapat mendeteksi terhadap serangan yang baru, tetapi dibalik itu semua metode ini bisa menghasilkan sedikitnya *false alarm*.

b. *Anomaly Based*

Deteksi yang melakukan cara analisis terhadap perilaku atau *behavior* pada sebuah lalu lintas jaringan, jadi akan bisa membedakan antara perilaku aktivitas normal dan aktivitas serangan.

2.6 *Man In The Middle* (MITM)

Serangan MITM adalah serangan dimana penyerang secara diam-diam mencegat dan menyampaikan pesan antara dua pihak yang yakin bahwa mereka sedang berkomunikasi secara langsung satu sama lain [17]. Serangan MITM dilakukan dengan membuat koneksi terpisah antara penyerang dan target, kemudian menyampaikan paket transmisi sehingga membuat target percaya bahwa mereka sedang terhubung ke internet secara langsung, sedangkan sebenarnya proses komunikasi yang dilakukan target sedang dimanipulasi oleh penyerang.

2.6.1 Jenis MITM

Berdasarkan [18] MITM dibagi menjadi beberapa jenis, yaitu:

2.6.1.1 Spoofing Based MITM Attack

Serangan *spoofing* melibatkan peniruan identitas pengguna atau perangkat apapun di jaringan oleh pihak jahat. Ada empat jenis utama serangan *spoofing*, yaitu *ARP Spoofing*, *DHCP Spoofing*, *DNS Spoongfing*, dan *IP Spoofing*.

a. *ARP(Address Resolution Protocol) Spoofing*

Protokol ARP memetakan alamat jaringan ke alamat MAC. ARP adalah protokol tepercaya dan paling penting untuk komunikasi LAN. Musuh memodifikasi tabel cache ARP lokal dan mengaitkan alamat MAC host dengan IP target. Serangan MITM dilakukan untuk mendapatkan akses ke rahasia pengguna informasi.

b. *DNS Spoofing*

Nama domain dari server DNS diatur atau diubah ke dalam domain level yang lebih rendah, subordinat, dan domain level yang lebih tinggi. Sehingga

klien yang membuka domain tersebut membuka dns yang diatur ke situs penyerang.

c. *DHCP spoofing*

Protokol DHCP bertanggung jawab untuk menyediakan parameter konfigurasi jaringan untuk host baru. Parameter ini termasuk *subnet mask*, *DNS server*, *default gateway*, leased time, dan alamat IP.

d. *IP spoofing*

Dalam serangan *spoofing IP*, musuh jahat menyadap komunikasi antara pihak yang sah. Musuh ini mengontrol arus komunikasi dan menghilangkan informasi yang dikirim oleh pihak asli tanpa sepengetahuan titik akhir asli.

2.6.1.2 TSL/SSL MITM Attack

Secure Socket Layer (SSL) dan *Transport Layer Security* (TLS) adalah enkripsi protokol yang menyediakan data aman, transfer dan komunikasi memalui internet. Membuat saluran komunikasi yang aman antara dua pihak (klien dan server). Serangan MITM SSL/TSL adalah penyerang berada di tengah antara dua pihak perangkat yang sedang berkomunikasi dan membuat dua koneksi SSL secara terpisah, dan menyampaikan pesan diantara perangkat.

2.6.1.3 BGP (Border Gateway Protoco) Based MITM Attack

BGP adalah protokol *routing* internet inti yang memfasilitasi pemilihan jalur tercepat. Serangan MITM terkait BGP ini berdasarkan IP *hijacking* dan karenanya kadang-kadang dikenal sebagai BGP *hijacking* atau *prefix hijacking* atau *route hijacking*.

2.6.1.4 FBS (False Base Station) Based MITM Attack

FBS adalah serangan dimana musuh menyamar sebagai *base station transceiver*. BTS palsu dapat bertindak sebagai BTS asli dan menyiarkan sinyal BTS melalui udara dan dengan demikian membuat perangkat di area tersebut berkomunikasi dengannya.

a. *GSM based MITM attack*

Serangan MITM berbasis GSM arsitektur GSM terdiri dari BTS dan stasiun bergerak dan berkomunikasi satu sama lain melalui tautan radio. BTS terhubung dengan tautan pengontrol stasiun pangkalan untuk pusat pengalihan seluler yang mengarahkan sinyal ke jaringan tetap apapun.

b. *UMTS based MITM attack*

UMTS adalah penerus GSM dan memberikan kepastian perangkat tambahan untuk menghilangkan kerentanan. GSM mendukung enkripsi dan otentikasi pelanggan dari antarmuka radio antara BTS dan MS. UMTS menyediakan penyempurnaan dan fitur tambahan seperti perlindungan integritas lalu lintas sinyal dan token otentikasi.

2.7 *Synthetic Minority Oversampling Technique* (SMOTE)

Ketidakseimbangan pada dataset mengakibatkan buruknya kapasitas *machine learning.* Untuk menyeimbangkan data tersebut bisa diselesaikan dengan teknik *oversampling.* Teknik *oversampling* adalah menambah jumlah sampel kelas minoritas dengan cara menyalin secara acak sampel minoritas, sehingga dapat menyeimbangkan ukuran *sample* kelas minoritas dan kelas mayoritas. SMOTE adalah salah satu metode *oversampling* yang paling umum digunakan untuk memecahkan masalah ketidakseimbangan [19].

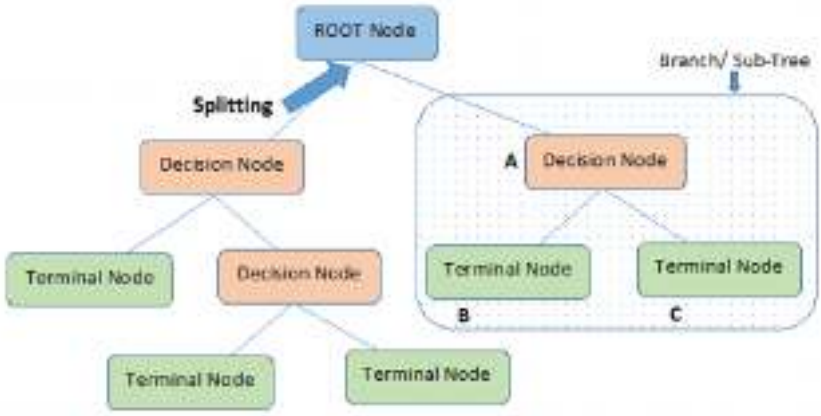
2.8 *Random Under Sampling*

Untuk mengatasi ketidakseimbangan bukan hanya bisa menggunakan *oversampling.* Teknik lainnya untuk mengatasi ketidakseimbangan data juga bisa menggunakan teknik *undersampling. Random Undersampling (RUS)* adalah metode untuk menghitung perbedaan antara kelas mayoritas dan minoritas, data mayoritas dihapus secara acak, sehingga kelas mayoritas sama dengan minoritas [20]. Namun, kelemahan utama dari *undersampling* adalah bisa saja data yang penting diabaikan dan ikut terhapus.

2.9 Algoritma *Decision Tree*

Decision tree adalah teknik dalam klasifikasi yang digunakan untuk mentedeksi intusi berbasis anomali dan intrusi berbasis web. *Decision tree* disebut "*tree*" karena memang mempunyai struktur seperti pohon yang terbalik, dimana setiap simpul menunjukkan tes, masing-masing cabang mewakili hasil tes, dan setiap simpul daun (*terminal node*) memegang label kelas. Algoritma ini digunakan dalam *machine learning* dan pengenalan pola, ada berbagai algoritma dalam pohon keputusan yaitu ID3, C4.5 dan CART [21].

Decision tree adalah suatu metode algoritma yang digunakan untuk teknik klasifikasi dan regresi yang mana keduanya mempunyai tujuan untuk melakukan prediksi terhadap sekumpulan data. Perbedaan dari kedua teknik ini adalah teknik prediksi, dimana klasifikasi itu menggunakan nilai diskrit sedangkan regresi memakai nilai kontinu. Selanjutnya perbedaan terhadap metode dalam perhitungan, pada klasifikasi dengan mengukur akurasi sedangkan regresi dengan pengukuran *root mean square*.



Gambar 2.7 Struktur *Decision Tree*

2.10 Evaluasi Performa Metode *Decision Tree*

Untuk mengukur kinerja akurasi dari sistem deteksi bisa menggunakan metode *Confusion matrix.*

Tabel 1 *Confusion Matrix* [22]

	Prediccted Attack	*Predicted normal*
Actual Acctack	**TP**	**FP**
Actual Normal	**FN**	**TN**

Tabel 2 *Alert Confusion Matrix*

No	Tipe Alert	Definisi
1.	*True Positive* (TP)	Traffic terdeteksi serangan
2.	*False Positive* (FP)	Traffic normal namun terseteksi serangan
3.	*False Negative* (FN)	Traffic normal
4.	*True Negative* (TN)	Traffic serangan namun terdeteksi normal

Untuk mengukur performa dapat dilakukan penghitungan *accuracy, false alarm rate, detection rate*, dan *precision*.

$$Accuracy = \frac{TP+TN}{TP+TN+FP+FN} \quad (1)$$

$$TPR = \frac{TP}{TP+FN} \quad (2)$$

$$FPR = \frac{FP}{TN+FP} \quad (3)$$

$$TNR = \frac{TN}{TN+FP} \quad (4)$$

$$FNR = \frac{FN}{FN+TP} \quad (5)$$

$$Precision = \frac{\mathrm{TP}}{\mathrm{TP+FP}} \quad (6)$$

BAB III

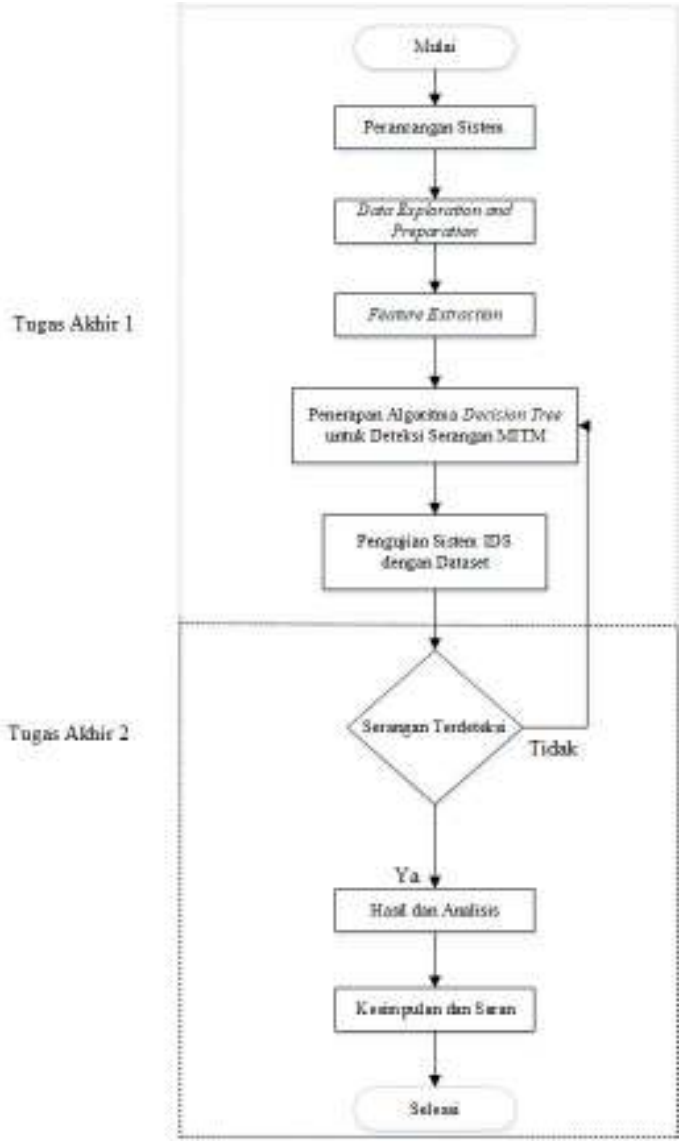
METODOLOGI PENELITIAN

3.1 Pendahuluan

Pada bab ini berisi mengenai urutan penelitian tugas akhir. Metodologi penelitian dirancang untuk mendeteksi serangan *Man in The Middle Attack* dan membedakannya dengan paket normal pada *Supervisory Control and Data Acquisition* menggunakan *Decision Tree*. Dimana untuk mencapai itu pada penelitian ini memiliki beberapa tahapan yang nantinya dijelaskan pada kerangka kerja penelitian tugas akhir ini.

3.2 Kerangka Kerja Penelitian

Tahap pertama yaitu perancangan sistem, dengan melakukan ekstraksi dataset dari format pcap menjadi CSV (*Comma Separated Values*). Tahap selanjutnya adalah mencari fitur yang dibutuhkan untuk melakukan pengenalan dan pencarian pola serangan MITM. Kemudian hasil ekstraksi tersebut diolah dan dibuat program untuk mentedeteksi serangan dengan algoritma *decision tree.* Program yang telah dibuat kemudian diuji coba dan diukur akurasinya dalam mendeteksi serangan MITM tersebut. Berikut diagram air untuk kerangka kerja penelitian tugas akhir:



Gambar 3.1 Kerangka Kerja

3.3 Perancangan Sistem

Sistem akan dibuat dengan algoritma *Decision Tree* sebagai *Network Instrusion Detection System* (NIDS) untuk mendeteksi serangan *Man in The Minddle*. Pertama, file dataset pcap dibaca oleh sistem dan akan mengambil informasi penting. Tahap selanjutnya sistem akan melakukan NIDS dengan metode *Decision Tree* untuk mendeteksi MITM. Setelah terdeteksi hasil deteksi akan akan dianalisa akurasinya dengan menggunakan confusion matrix.

3.3.1 Perangkat Penelitian

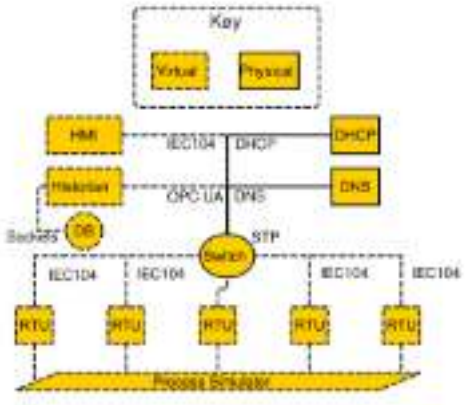
Pada penelitian tugas akhir ini terdapat beberapa kebutuhan perangkat lunak dan perangkat keras. Tabel di bawah ini akan menerangkan tentang spesifikasi perangkat yang digunakan dalam penelitian tugas akhir **:**

Tabel 3 Perangkat Penelitian.

No	Perangkat Lunak	Perangkat Keras
1	Wireshark	Laptop Acer A514-51G-59HF
2	Snort	
3	Vscode	
4	Phyton	
5	Tshark	

3.4 Dataset *Testbet*

Dataset pada penelitian ini merupakan dataset yang dikembangkan pada penelitian [23] “, dataset tersebut berisi gabungan antara data normal dan juga data serangan. Data tersebut diterbitkan pada tahun 2018 dan tersedia dalam bentu .pcap dan .rw. Dataset dibangun dengan menggunakan 9 *host* yang terdiri dari : 1x HMI; 1x *Data Historian*; 5 RTU; 1x MITM *attacker,* dan 1x *Reconnaissance.* Dataset terdiri dari beberapa *feature* yang berfungsi sebagai sampel boostrap dan 2 kelas sebagai *output* .Dataset tersebut dipublikasikan di internet yaitu “https://figshare.com/articles/dataset/dataset-v1_pcap/6133457/1”



Gambar 3.2 Diagram *Network Testbed*

3.5 Deteksi Serangan dengan Menggunakan *Snort* IDS

Snort IDS akan digunakan untuk mendeteksi serangan yang ada di dataset pcap, ini dilakukan untuk mengetahui apakah serangan yang digunakan pada penelitian ini terpadat pada dataset pcap tersebut. Hasil deteksi tersebut akan disimpan dalam bentuk *log alert*, semua jenis serangan yang terdapat pada *rule snort* akan terdeteksi, bukan hanya serangan yang akan dijadikan objek penelitian ini.

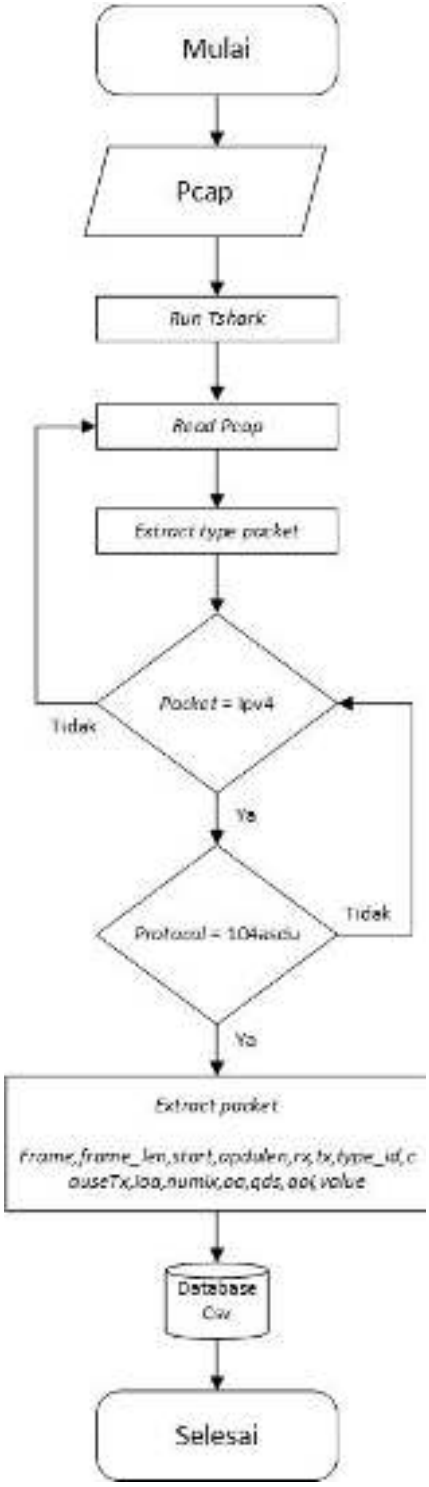
Gambar 3.3 *Flowchart Snort* IDS

3.6 Data *Filtering*

Tahap ini adalah tahap dimana dataset akan difilter terlebih dahulu sebelum dataset itu akan diekstraksi. Dengan melalukan filter, selain protokol IEC 104 pada data akan dihapus yang tidak diperlukan dan hanya akan menyisikan paket IEC 104.

3.7 Data *Extraction*

Tahap ini dilakukan untuk proses mengambil nformasi yang dibutuhkan untuk mengenali paket serangan dengan paket yang lainnya. Data yang sebelumnya berbentuk pcap akan diubah format *Comma Sevared Value* (CSV).



Gambar 3.4 *Flowchart Extraction*

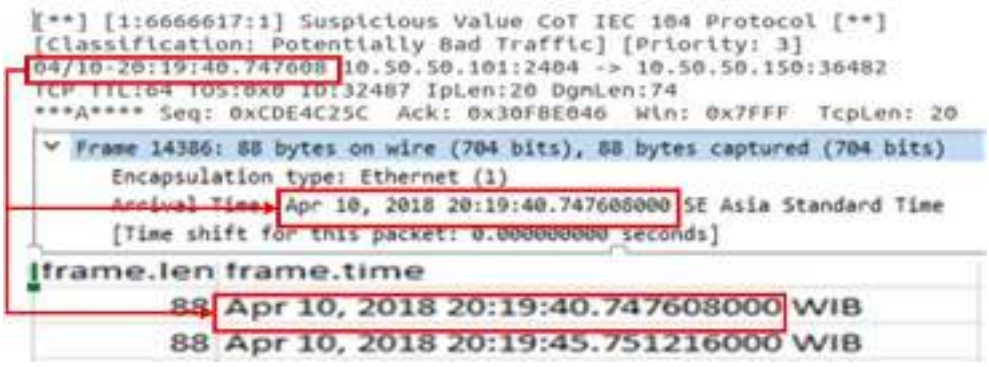
Pada data *extraction* protokol IEC 104 terdiri dari atribut-atribut yang akan digunakan mengekstrak dataset normal dan serangan *Man in The Middle*. Atribut-atribut yang diekstrak adalah sebagai berikut:

Tabel 4 Atribut *Extraction Protocol* IEC 104

No	Atribut IEC 104
1	Frame
2	frame_len
3	start
4	apdulen
5	rx
6	tx
7	type_id
8	causeTx
9	ioa
10	numix
11	oa
12	qds
13	qoi
14	value

3.8 Mencari Pola Serangan *Man In The Middle*

Salah satu cara mengidentifikasi serangan adalah dengan pola. Serangan biasanya berpola berupa karatekristik yang unik yang terdapat di paket data. Pola serangan pada penelitian ini digunakan sebagai klasifikasi algoritma *Decision Tree* dalam menentukan apakah terdapat serangan atau tidak. Untuk mendapatkan pola serangan akan dilukakan dengan korelasi antara *raw* data, *snort alert*, dan data ekstraksi.

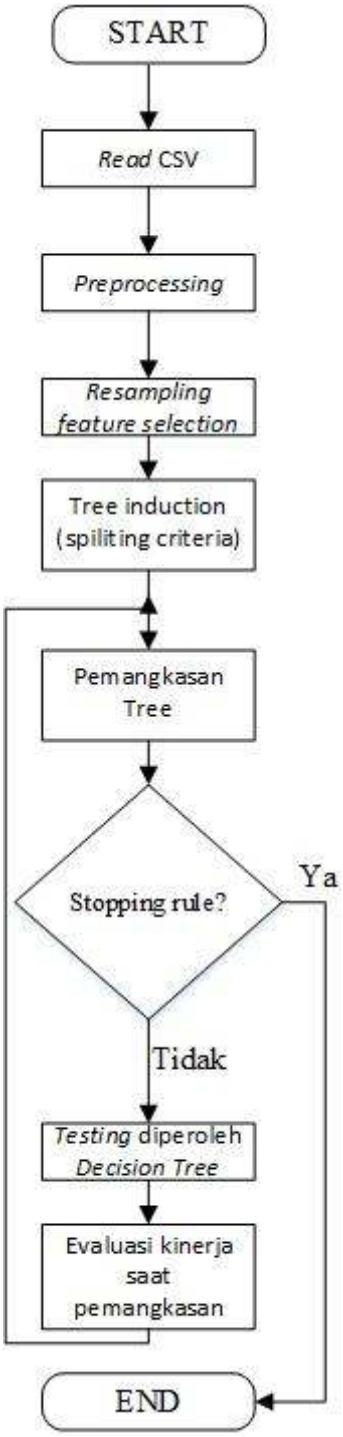


Gambar 3.4 Hubungan Antara *raw* data, *snort alert*, dan data ekstraksi

3.9 Decision Tree

Decision Tree adalah pengklasifikasi yang dianggap sebagai metode yang paling terkenal untuk representasi klasifikasi data pengklasifikasi. Pengklasifikasi *decision tree* dikenal karena tampilannya yang disempurnakan dari hasil kinerja karena presisi dan akurasi yang kuat [24]. Pada penelitian ini akan diterapkan model klasifikasi *decision tree* untuk mendeteksi serangan dengan akurasi yang tinggi.

Flow chart untuk algoritma *decision tree* akan ditunjukan oleh gambar 3.4. *Flow chart* tersebut akan menunjukkan beberapa tahapan dalam proses program *decision tree.* Pada saat *decision tree* mulai membaca dataset yang berbentuk data csv maka dilakukan proses *preprocessing* dan selanjutnya *feature selection* dimana proses ini merupakan proses menyiapkan data sebelum diolah *decision tree* tersebut. Proses selanjutnya adalah *splitting criteria,* dan selanjutnya adalah proses *tree pruning* yaitu proses pemangkasan data yang merupakan salah satu proses pembentukan *decision tree*. Dan proses hingga selanjutnya untuk proses program *decision tree*.



Gambar 3.5 *Flowchart Program Decision Tree*

BAB IV

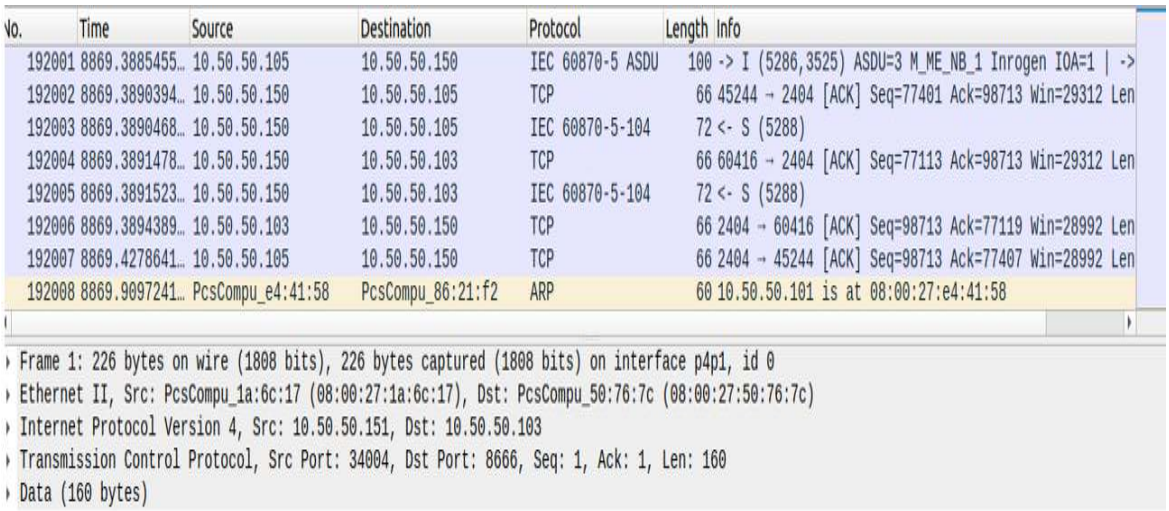
HASIL DAN ANALISIS

4.1 Pendahuluan

Pada bab ini akan menjelaskan tentang pengujian dari penelitian ini. Pengujian tersebut dilakukan dengan beberapa tahapan. Tahapan pertama adalah melakukan validasi atau kecocokan antara dataset hasil ekstraksi dan dataset pcap (*raw data*) sehingga mendapatkan pola serangan. Tahapan selanjutnya adalah penerapan algoritma *Decision Tree* untuk mendeteksi serangan Man In The Middle pada dataset *Scada*

4.2 *Raw* Dataset

Penelitian ini menggunakan dataset yang dibangun menggunakan Tetsbed SCADA yang diambil dari internet. Dataset ini ada beberapa protkol jaringan yaitu TCP, IEC-104 ASDU, IEC-104 APCI, Tlsv1.2, ARP, SSH yang nantinya akan difilter dan akan menyisakan protocol IEC-104. Dataset gabungan ini terdiri dari 192.008 baris paket data dengan besar file 36.56MB. Adapun bentuk dataset pcap dapat dilihat pada gambar 4.1.



No.	Time	Source	Destination	Protocol	Length	Info
192001	8869.3885455…	10.50.50.105	10.50.50.150	IEC 60870-5 ASDU	100	-> I (5286,3525) ASDU=3 M_ME_NB_1 Inrogen IOA=1 | ->
192002	8869.3890394…	10.50.50.150	10.50.50.105	TCP	66	45244 → 2404 [ACK] Seq=77401 Ack=98713 Win=29312 Len
192003	8869.3890468…	10.50.50.150	10.50.50.105	IEC 60870-5-104	72	<- S (5288)
192004	8869.3891478…	10.50.50.150	10.50.50.103	TCP	66	60416 → 2404 [ACK] Seq=77113 Ack=98713 Win=29312 Len
192005	8869.3891523…	10.50.50.150	10.50.50.103	IEC 60870-5-104	72	<- S (5288)
192006	8869.3894389…	10.50.50.103	10.50.50.150	TCP	66	2404 → 60416 [ACK] Seq=98713 Ack=77119 Win=28992 Len
192007	8869.4278641…	10.50.50.105	10.50.50.150	TCP	66	2404 → 45244 [ACK] Seq=98713 Ack=77407 Win=28992 Len
192008	8869.9097241…	PcsCompu_e4:41:58	PcsCompu_86:21:f2	ARP	60	10.50.50.101 is at 08:00:27:e4:41:58

```
Frame 1: 226 bytes on wire (1808 bits), 226 bytes captured (1808 bits) on interface p4p1, id 0
Ethernet II, Src: PcsCompu_1a:6c:17 (08:00:27:1a:6c:17), Dst: PcsCompu_50:76:7c (08:00:27:50:76:7c)
Internet Protocol Version 4, Src: 10.50.50.151, Dst: 10.50.50.103
Transmission Control Protocol, Src Port: 34004, Dst Port: 8666, Seq: 1, Ack: 1, Len: 160
Data (160 bytes)
```

Gambar 4.1 Dataset pcap

4.3 Serangan MITM

Serangan yang terdapat pada dataset adalah *Arp Spoofing* yang dilakukan ke HMI . Sebelum dilakukan serangan MITM pada target dilakukan beberapa proses seperti melakakukan *network scanning* pada HMI yang bertujuan untuk mengetahui ip dan port

yang terhubung pada HMI yang memungkinkan penyerang dapat masuk ke sana. Kemudian penyerang akan menyamar sebagai salah satu RTU yang dimana RTU ini akan merubah nilai COT menjadi invalid. COT sendiri merupakan suatu elemen pada protokol IEC 104 dimana didalamnya berisi suatu informasi, contohnya saja ketika suatu HMI mengirim suatu interrogation command dengan kode C_IC_NA_1 maka RTU akan menjawab pesan dari HMI dengan respon M_MB_NB_1 yang berarti RTU melakukan pembacaan nilai simulasi. Hal ini juga mendasari pada penggunaan dataset pada proses machine learning protokol yang digunakan hanya IEC 104

4.4 Snort sebagai IDS

Pengujian raw data dengan snort ids untuk membuktikan bahwa pada raw data yang digunakan terdapat sebuah serangan. Sebelum snort mengeluarkan output berupa alert, sebelumnya snort perlu dikonfigurasi terlebih dahulu. Konfigurasi yang dilakukan adalah dengan mengaktifkan rules-rules yang berhubungan dengan serangan agar Snort dapat mendeteksi serangan dengan benar. Rules yang digunakan pada penelitian ini adalah sebagai berikut :

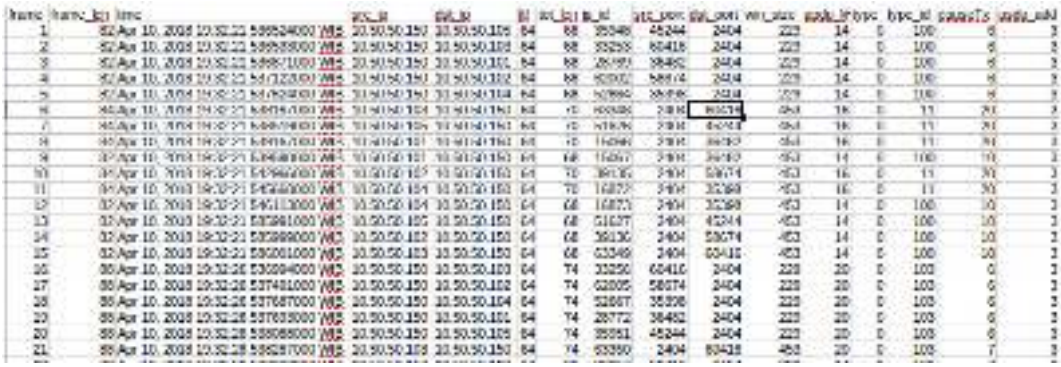
Tabel 5 *Rules Snort*

No	Rules
1	local.rules

Gambar 4.2 *Log Alert* Snort IDS

4.5 Ekstraksi Dataset

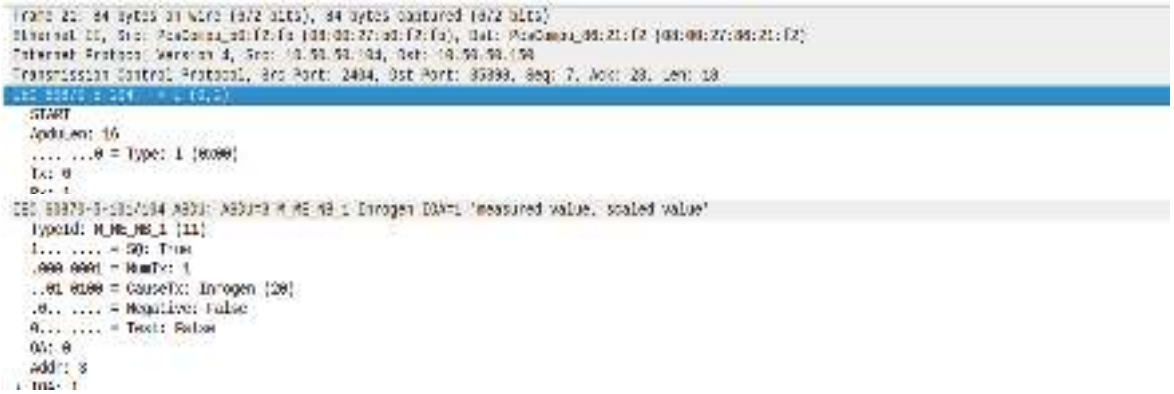
Dataset pcap akan diekstraksi ke dalam bentuk CSV (*Comma Separted Value*) agar data dapat berupa angka yang dapat dibuka dengan microsoft excel. Data CSV itulah yang akan digunakan dan diolah ke pemograman *machine learning* dengan algoritma *Decision Tree.*



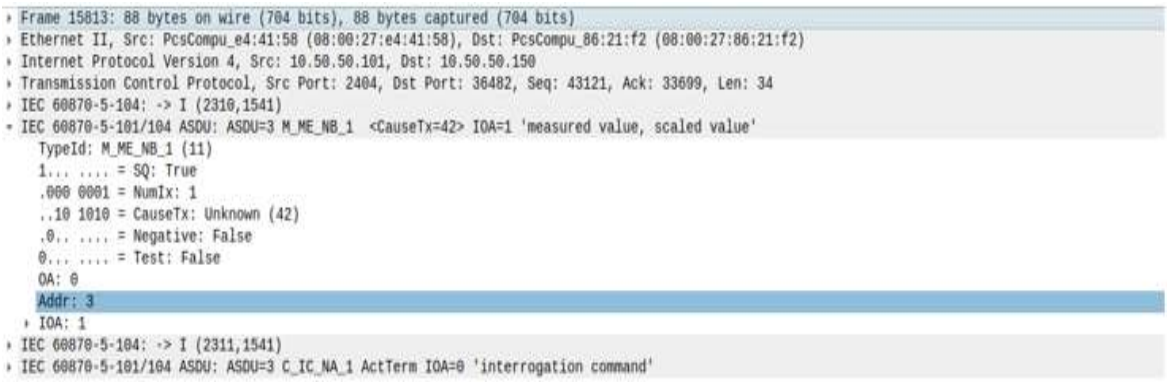
Gambar 4.3 Dataset CSV

4.6 Pengenalan Pola Serangan

Tahapan ini akan berisi Analisa dari dataset yang berfokus pada *payload* protokol IEC-104 dikarenakan serangan ini tertuju pada *transfort layer* dan *data link layer* yang mempunyai hubungan langsung dengan komunikasi jaringan SCADA. Berikut adalah sampel paket normal dan serangan pada penelitian ini.



Gambar 4.4 Paket Normal IEC 104



Gambar 4.5 Paket Serangan MITM IEC 104

Pada gambar 4.3 dan Gambar 4.4 menunjukkan aktifitas trafik normal dan serangan pada taset pcap. Saat trafik normal memiliki *payload CauseTx Inrogen*, sedangkan pada trafik serangan memiliki *payload CauseTx unknown.* Pada trafik normal juga memiliki panjang data 84 byte sedangkan trafik serangan memiliki Panjang data 88 byte.

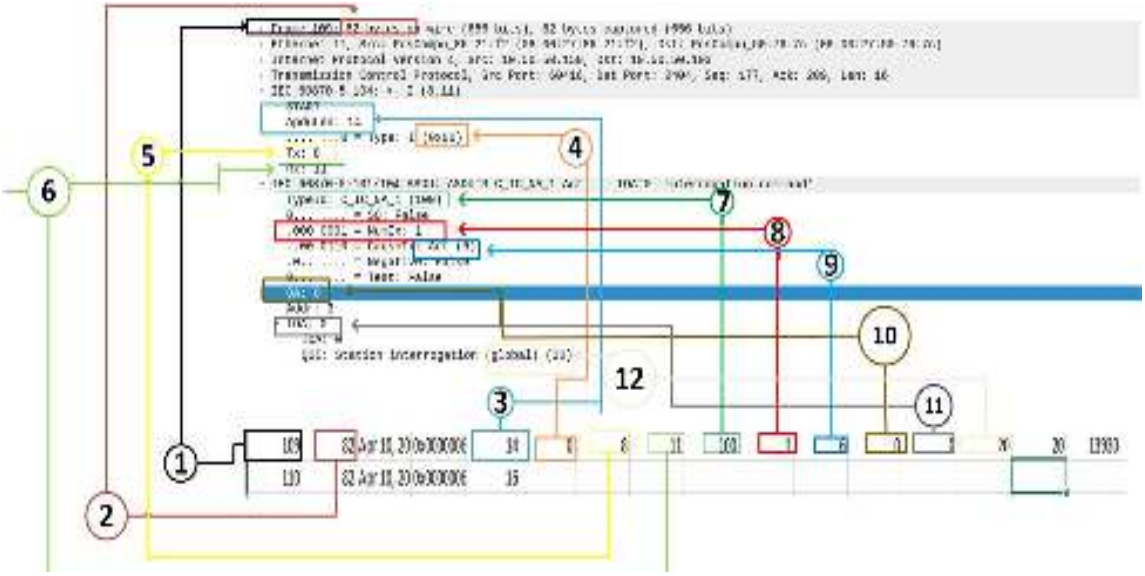
Pada [14] dijelaskan bahwa M_ME_NB_1 <CauseTx=42> IOA=1 ‘measured value, scaled value’ pada *payload* diatas nilai CauseTx=42 adalah invalid, itu disebebkan karena untuk TypeId M_ME_NB_1 nilai CauseTx yang valid adalah 2,3,5,11,12,20,20+G.

Type	Description	Reference	Format	Valid COTs
Process information in monitor direction :				
1	Single point information	M_SP_NA_1	SIQ	2,3,5,11,20,20+G
2	Single point information with time tag	M_SP_TA_1	SIQ + CP24Time2a	3,5,11,12
3	Double point information	M_DP_NA_1	DIQ	2,3,5,11,12,20,20+G
4	Double point information with time tag	M_DP_TA_1	DIQ + CP24Time2a	3,5,11,12
5	Step position information	M_ST_NA_1	VTI + QDS	2,3,5,11,12,20,20+G
6	Step position information with time tag	M_ST_TA_1	VTI + QDS + CP24Time2a	2,3,5,11,12
7	Bit string of 32 bit	M_BO_NA_1	BSI + QDS	2,3,5,11,12,20,20+G
8	Bit string of 32 bit with time tag	M_BO_TA_1	BSI + QDS + CP24Time2a	3,5
9	Measured value, normalized value	M_ME_NA_1	NVA + QDS	2,3,5,11,12,20,20+G
10	Measured value, normalized value with time tag	M_ME_TA_1	NVA + QDS + CP24Time2a	3,5
11	Measured value, scaled value	M_ME_NB_1	SVA + QDS	2,3,5,11,12,20,20+G
12	Measured value, scaled value with time tag	M_ME_TB_1	SVA + QDS + CP24Time2a	3,5
13	Measured value, short floating point value	M_ME_NC_1	IEEE STD 754 + QDS	2,3,5,11,12,20,20+G
14	Measured value, short floating point value with time tag	M_ME_TC_1	IEEE STD 754 + QDS + CP24Time2a	2,3,5,11,12,20,20+G
15	Integrated totals	M_IT_NA_1	BCR	2,37,37+G
16	Integrated totals with time tag	M_IT_TA_1	BCR + CP24Time2a	3,37,37+G
17	Event of protection equipment with time tag	M_EP_TA_1	CP16Time2a + CP24Time2a	3
18	Packed start events of protection equipment with time tag	M_EP_TB_1	SEP + QDP +C P16Time2a + CP24Time2a	3
19	Packed output circuit information of protection equipment with time tag	M_EP_TC_1	OCI + QDP + CP16Time2a + CP24Time2a	3
20	Packed single-point information with status change detection	M_PS_NA_1	SCD+QDS	2,3,5,11,12,20,20+G
21	Measured value, normalized value without quality descriptor	M_ME_ND_1	NVA	1,2,3,5,11,12,20,20+G

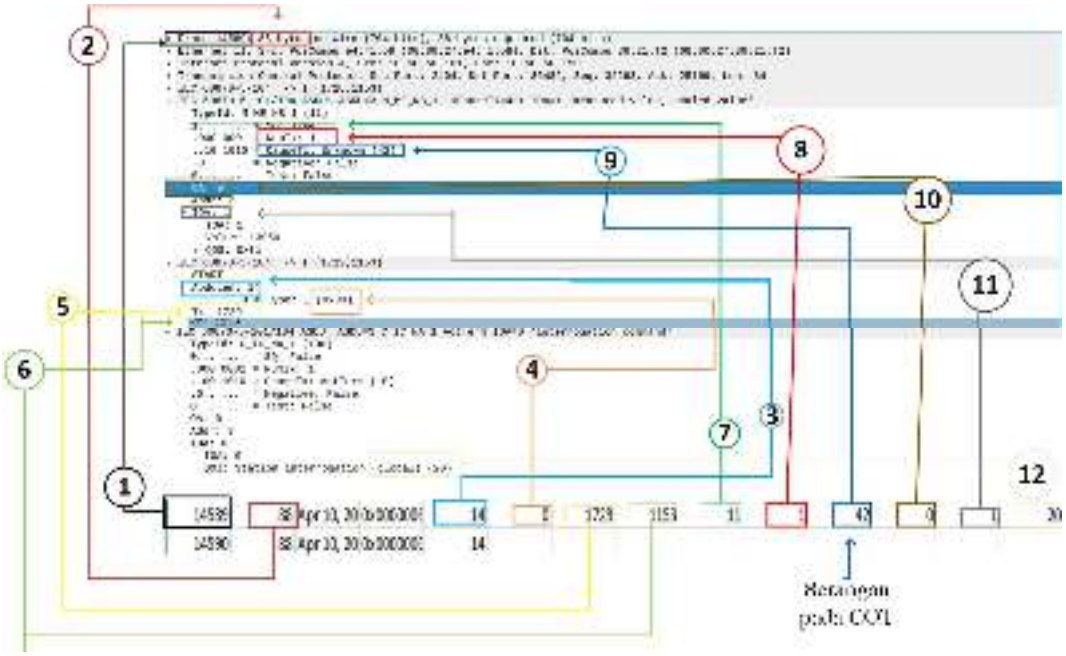
Gambar 4.6 IEC 104 ASDU *Types*

4.7 Hasil Data Ekstraksi

Data hasil ekstraksi dengan file pcap perlu divalidasi. Pada tahapan ini adalah pembuktian bahwa memang dataset ekstraksi dan data *raw* adalah data yang sama. Pada gambar 4.6 akan membandingkan data hasil ekstraksi dan file pcap.



Gambar 4.7 Perbandingan Hasil Ekstraksi Data IEC 104 Normal



Gambar 4.8 Perbandingan Hasil Ekstraksi Data IEC 104 Serangan

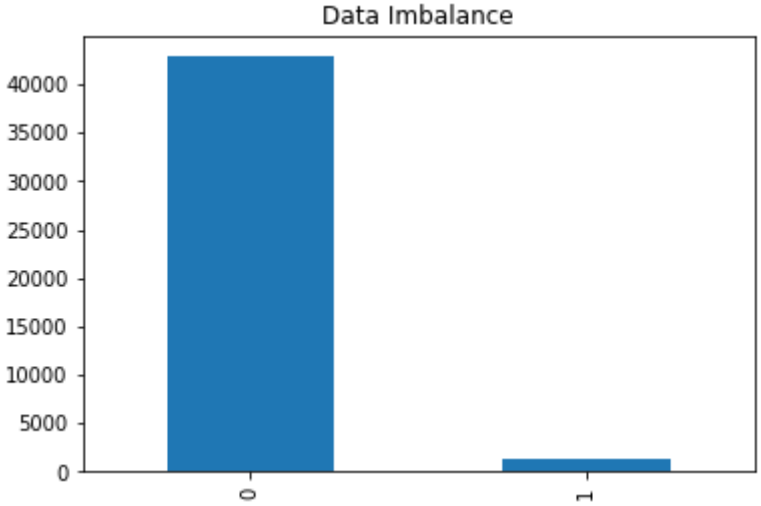
Pada gambar 4.7 dan 4.8 korelasi antara data ekstraksi dan raw data memiliki 12 features yang sama, yaitu:

1. Frame number (Nomor Frame).
2. Frame length (Panjang Frame).
3. 104.apci.apdulen (Panjang APDU).
4. Frame format APCI (Frame Format pada APCI).
5. 104apci.tx (Data Transfer).

6. 104apci.rx (Data Request).
7. 104asdu.typeid (*Type Identification* yang digunakan nomor, nomor 0 tidak digunakan, 1-127 digunakan untuk definisi standar IEC 101, 128-135 dicadangkan, dan 136-255 untuk penggunaan khusus).
8. 104asdu.numix. (Angka objek atau elemen nomor)
9. 104asdu.causeTx (*Cause Of Transmission* untuk mengontrol pengiriman pesan komunikasi jaringan nomor).
10. 104asdu.oa (Pengontrol konfirmasi perintah ke stasiun yang memberi perintah jika ada lebih dari *station* pengendali).
11. 104asdu.ioa (*Information Object Address* alamat informasi objek, nomor).
12. 104asdu.qoi (Kualitas deskripsi asdu dari sistem informasi *control direction*).

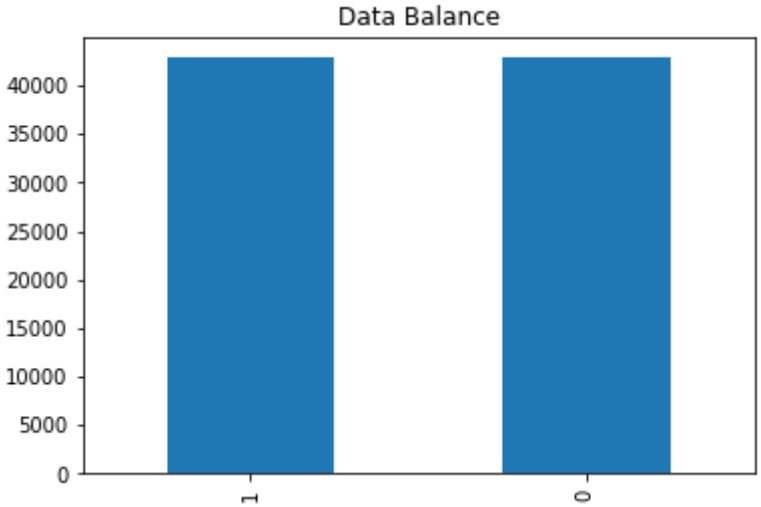
4.8 Oversampling Dataset

Teknik *oversampling* digunakan karena data yang tidak seimbang atau *imbalance*. Salah satu tenik *oversampling* adalah *Synthetic Minority Oversampling Technique* (SMOTE), tenik ini digunakan untuk *balancing* (menyeimbangkan) data minoritas dan mayoritas agar seimbang



Gambar 4.9 Data Sebelum SMOTE

Pada gambar diatas terlihat jelas data normal menjadi data kelas mayoritas dengan 42819 data, sedangkan data serangan menjadi kelas minoritas dengan jumlah 1253 data. Hal ini akan menjadi kendala karena data mayoritas akan lebih mudah dikenali daripada data minoritas

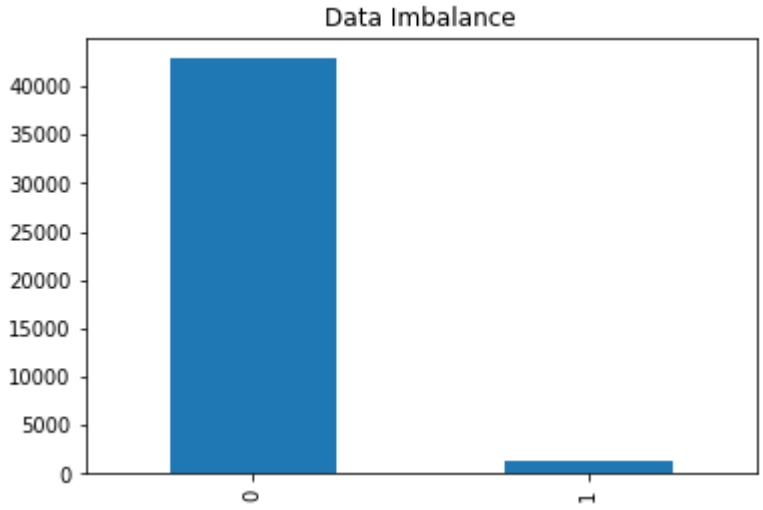


Gambar 4.10 Data Setelah SMOTE

Pada gambar diatas terlihat bahwa data serangan dan data normal telah seimbang dengan jumlah data yang sama yaitu 42819.

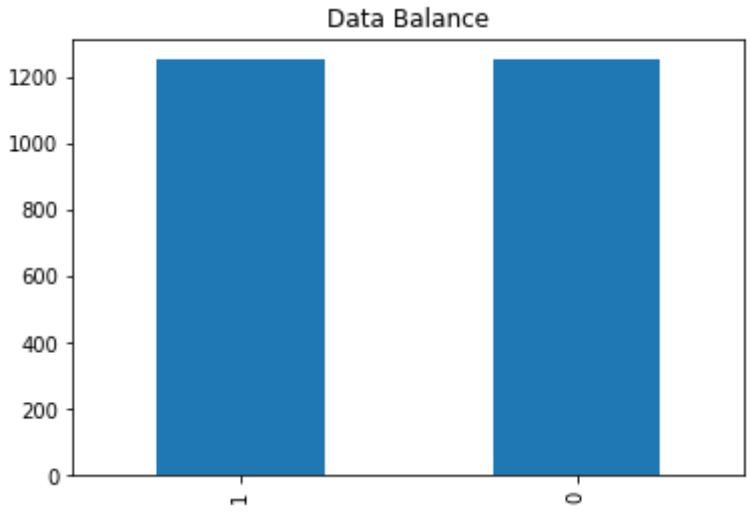
4.9 *Undersampling Dataset*

Teknik *undersampling* juga bisa digunakan untuk mengatasi masalah *imbalance* data. Salah satu Teknik undersampling adalah *Random Undersampling (RUS)*, *undersampling* digunakan untuk menyimbangkan data yang tidak seimbang.



Gambar 4.11 Data Sebelum RUS

Pada gambar diatas terlihat jelas data normal menjadi data kelas mayoritas dengan 42819 data, sedangkan data serangan menjadi kelas minoritas dengan jumlah 1253 data. Hal ini akan menjadi kendala karena data mayoritas akan lebih mudah dikenali daripada data minoritas



Gambar 4.12 Data Setelah RUS

Pada gambar diatas terlihat bahwa data serangan dan data normal telah seimbang dengan jumlah data yang sama yaitu 1253.

4.10 *Decision Tree*

Berikut merupakan *code* metode decision tree yang digunakan menggunakan dataset yang sudah melalui proses *sampling*

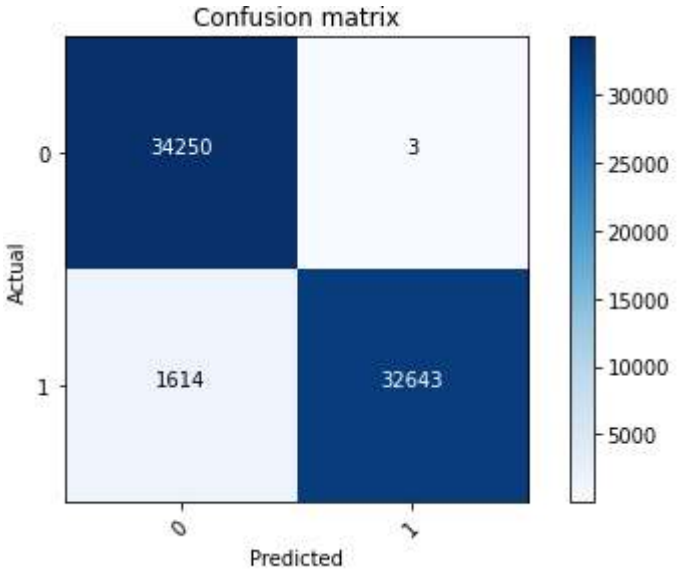
```
[ ]  from sklearn.tree import DecisionTreeClassifier
     model = DecisionTreeClassifier(max_depth=4,random_state=21)
     model.fit(X_train, y_train)

     DecisionTreeClassifier(max_depth=4, random_state=21)
```

Gambar 4.13 Decision Tree Code

4.11 Perhitungan *Confusion Matrix*

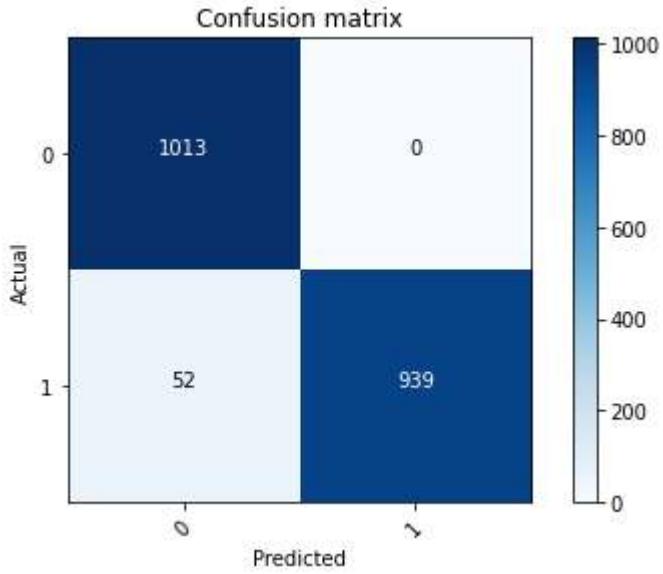
Perhitungan *confusion matrix* dengan nilai yang didapatkan pada confusion *matrix* yaitu *True Positive* (TP), *False Positive* (FP), *True Negative* (TN) dan *False Negative* (FN*). True Positive Rate* (TPR), *False Positive Rate* (FPR), *True Negative Rate* (TNR) dan *False Negatif Rate* (FNR)

1. **Data Training 80%**



Gambar 4.14 *Confusion Matrix Oversampling Training* 80%

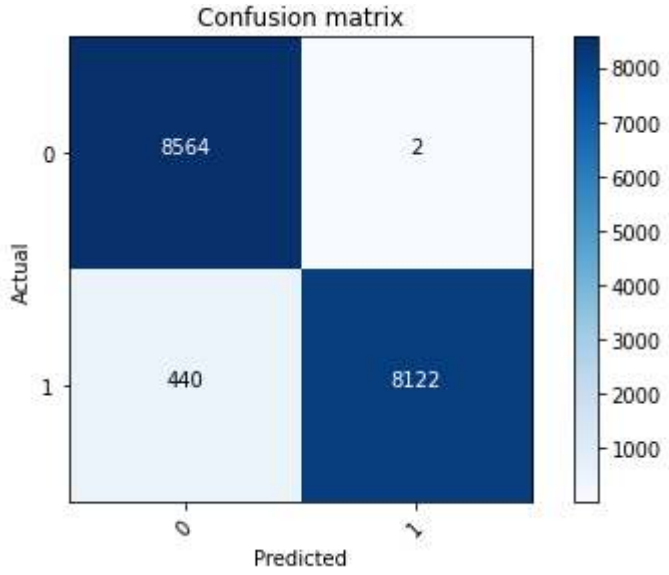
Pada *confusion matrix oversampling training* 80% menghasilkan *True Positive* (TP) 32643, *True Negative* (TN) 28551, *False Positive* (FP) 3, dan juga *False Negative* (FN) 1614.



Gambar 4.15 *Confusion Matrix Undersampling Training* 80%

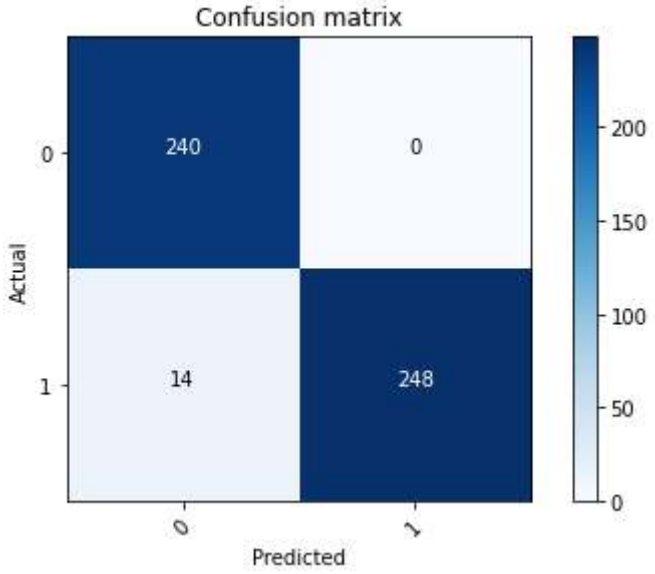
Pada *confusion matrix undersampling training* 80% menghasilkan *True Positive* (TP) 1013, *True Negative* (TN) 939, *False Positive* (FP) 0, dan juga *False Negative* (FN) 52.

2. Data Testing 20%



Gambar 4.16 *Confusion Matrix Oversampling Testing 2*0%

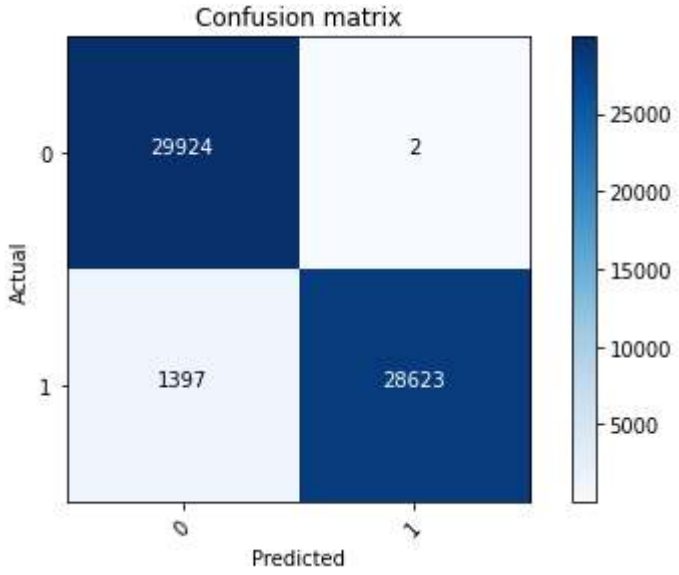
Pada *confusion matrix oversampling testing* 20% menghasilkan *True Positive* (TP) 8564, *True Negative* (TN) 8122, *False Positive* (FP) 2, dan juga *False Negative* (FN) 440.



Gambar 4.17 *Confusion Matrix Undersampling Testing 2*0%

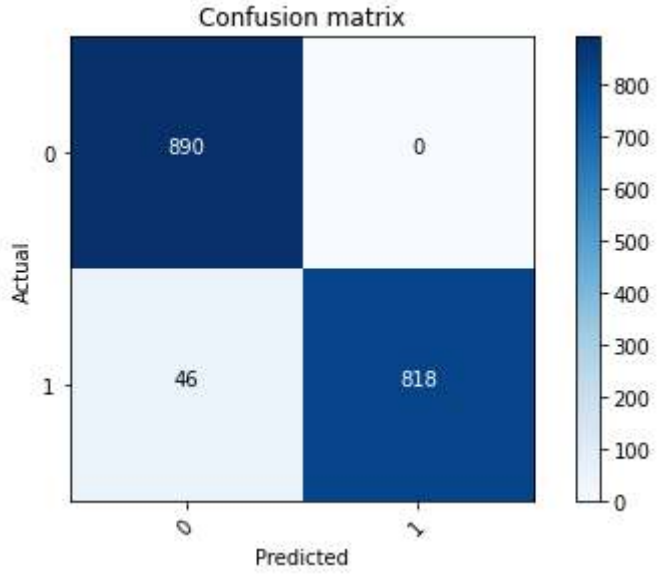
Pada *confusion matrix undersampling testing* 20% menghasilkan *True Positive* (TP) 240, *True Negative* (TN) 248, *False Positive* (FP) 0, dan juga *False Negative* (FN) 14.

3. Data Training 70%



Gambar 4.18 *Confusion Matrix Oversampling Training 7*0%

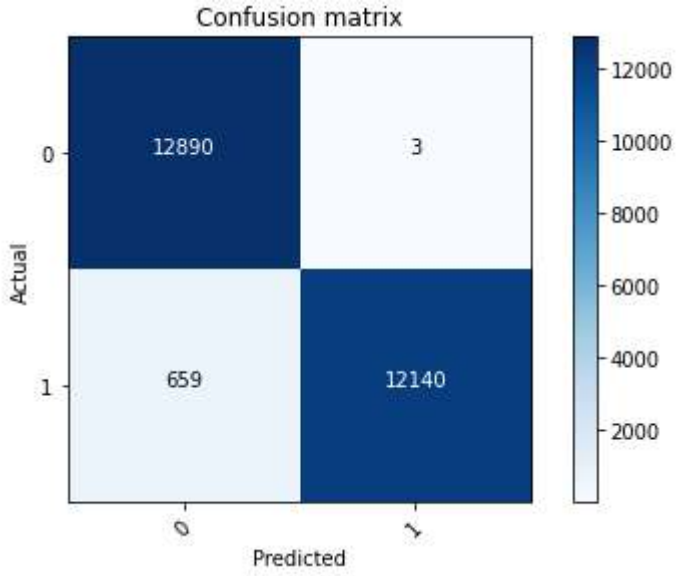
Pada *confusion matrix oversampling training* 70% menghasilkan *True Positive* (TP) 29924, *True Negative* (TN) 28623, *False Positive* (FP) 2, dan juga *False Negative* (FN) 1397.



Gambar 4.19 *Confusion Matrix Undersampling Training 7*0%

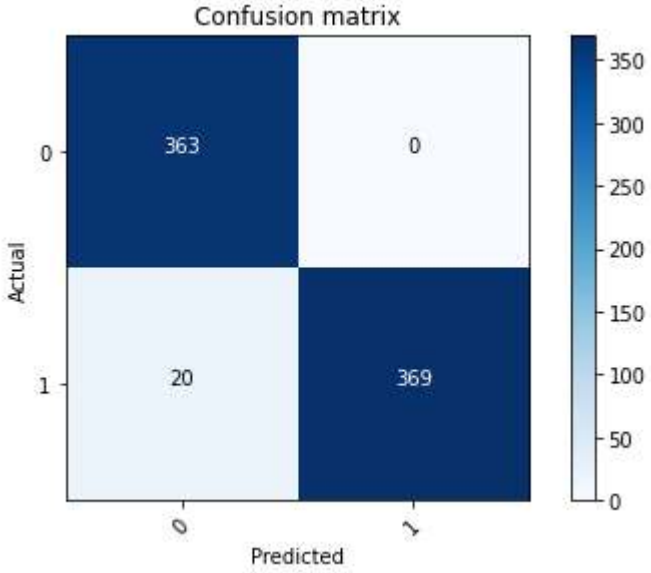
Pada *confusion matrix undersampling training* 70% menghasilkan *True Positive* (TP) 890, *True Negative* (TN) 818, *False Positive* (FP) 0, dan juga *False Negative* (FN) 46.

4. Data Testing 30%



Gambar 4.20 *Confusion Matrix Oversampling Testing 3*0%

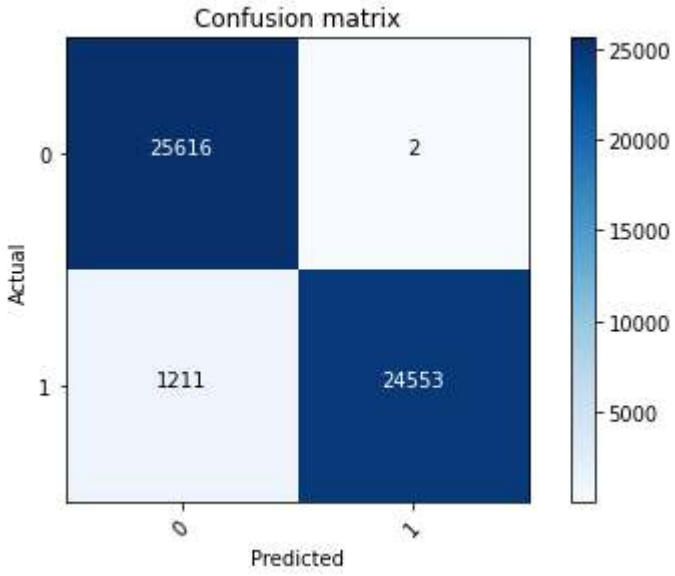
Pada *confusion matrix oversampling training* 30% menghasilkan *True Positive* (TP) 12890, *True Negative* (TN) 12140, *False Positive* (FP) 3, dan juga *False Negative* (FN) 659.



Gambar 4.21 *Confusion Matrix Undersampling Testing 3*0%

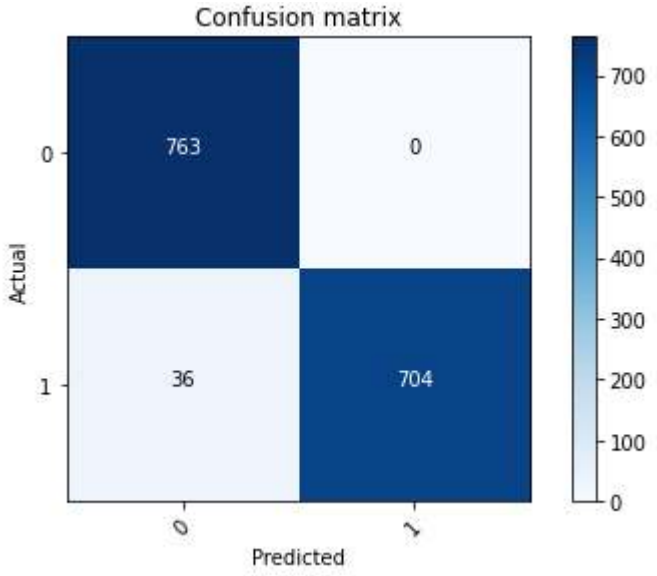
Pada *confusion matrix undersampling testing* 30% menghasilkan *True Positive* (TP) 363, *True Negative* (TN) 369, *False Positive* (FP) 0, dan juga *False Negative* (FN) 20.

5. Data Traning 60%



Gambar 4.22 *Confusion Matrix Oversampling Training* 60%

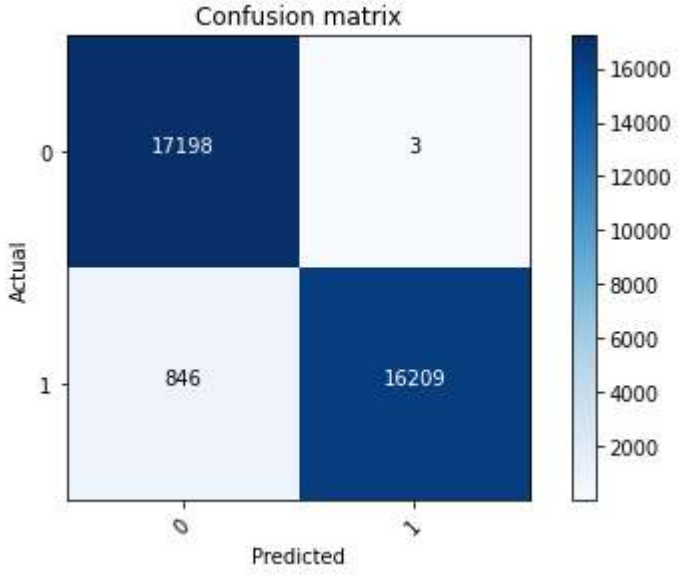
Pada *confusion matrix oversampling training* 60% menghasilkan *True Positive* (TP) 25616, *True Negative* (TN) 24553, *False Positive* (FP) 2, dan juga *False Negative* (FN) 1211.



Gambar 4.23 *Confusion Matrix Undersampling Training* 60%

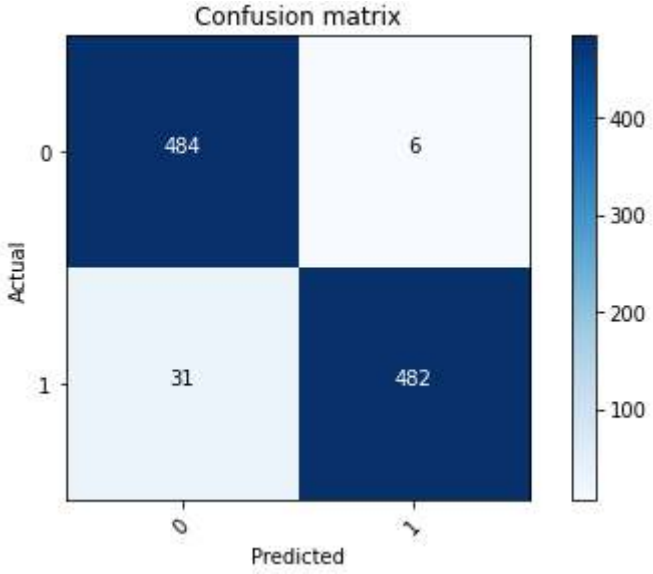
Pada *confusion matrix undersampling training* 60% menghasilkan *True Positive* (TP) 763, *True Negative* (TN) 704, *False Positive* (FP) 0, dan juga *False Negative* (FN) 36.

6. **Data Testing 40%**



Gambar 4.24 *Confusion Matrix Oversampling Testing* 40%

Pada *confusion matrix oversampling testing* 40% menghasilkan *True Positive* (TP) 17198, *True Negative* (TN) 16209, *False Positive* (FP) 3, dan juga *False Negative* (FN) 846.

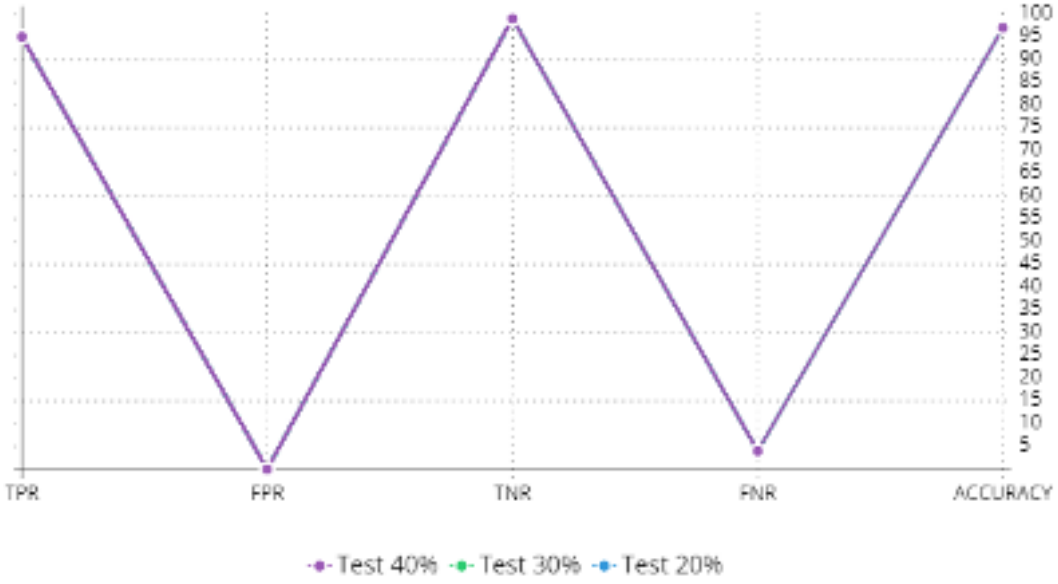


Gambar 4.25 *Confusion Matrix Undersampling Testing* 40%

Pada *confusion matrix undersampling training* 60% menghasilkan *True Positive* (TP) 484, *True Negative* (TN) 482, *False Positive* (FP) 6, dan juga *False Negative* (FN) 31.

Tabel 6 Hasil dengan *Oversampling*

Detection Rate	Training 80%, Testing 20%	Training 70%, Testing 30%	Training 60%, Testing 40%
TPR	95.14	95.13	95.31
FPR	00.02	00.02	00.01
TNR	99.97	99.97	99.98
FNR	04.88	04.86	04.68
Accuracy	97.41	97.42	97.52

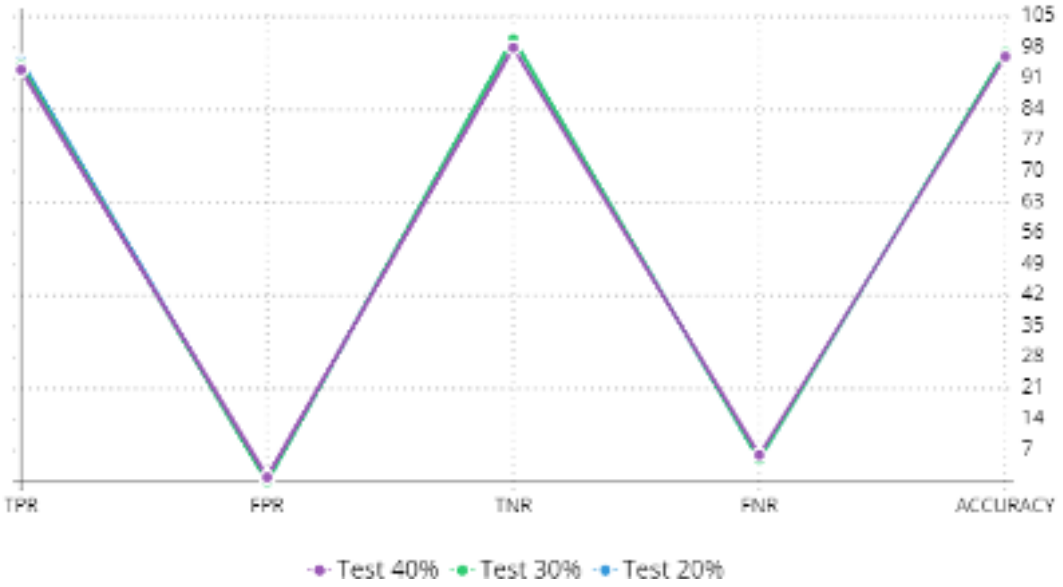


Gambar 4.26 Grafik hasil dengan *Oversampling*

Dari grafik tersebut menunjukkan perbandingan *detection rate* untuk setiap data *testing* 20%, 30% dan 40% berada pada skala nilai yang sama.

Tabel 7 Hasil dengan *Undersampling*

Detection Rate	Training 80%, Testing 20%	Training 70%, Testing 30%	Training 60%, Testing 40%
TPR	95.25	94.77	93.98
FPR	00.00	00.00	01.22
TNR	100.00	100.00	98.77
FNR	05.51	05.22	06.01
Accuracy	97.21	97.34	96.31



Gambar 4.27 Grafik hasil dengan *Undersampling*

Dari grafik tersebut menunjukkan perbandingan *detection rate* untuk setiap data *testing* 20%, 30% dan 40% berada pada skala nilai yang hampir sama.

Tabel dan grafk diatas yang merupukan hasil performa dari dataset yang telah melalui proses *oversampling* dan *undersampling*. Dari hasil tersebut data yang di*oversampling* memiliki keunggulan dari akurasi,TPR, dan FNR, namun data *undersampling* unggul dalam parameter FPR dan TNR. Dari table hasil diatas didapatkan performa terbaik dengan menggunakan metode *decision tree* yang didapat adalah menggunakan *oversampling* dengan *split data training* 60% dan testing 40%, yaitu dengan nilai performa:

Tabel 8 Hasil terbaik

TPR	FPR	TNR	FNR	*Accuracy*
95.31%	00.01%	99.98%	04.68	97.52

BAB V

KESIMPULAN DAN SARAN

5.1 Kesimpulan

Pada penelitian Tugas Akhir ini terdapat beberapa kesimpulan yang dihasilkan,yaitu :

1. Dalam dataset benar terdapat serangan MITM, dan algoritma *decision tree* bisa diimplementasikan untuk deteksi serangan MITM tersebut.
2. Untuk mengenali pola serangan MITM pada protokol IEC104, dapat dilihat dari *Cause of transmission* (*CauseTx*) dan panjang data.
3. Pendeteksian pada penelitian ini menggunakan *snort* sebagai acuan untuk mendeteksi serangan pada dataset, dan juga untuk perbandingan antara *raw data* dan hasil ekstraksi.
4. Serangan hanya terjadi pada protokol IEC-104 ASDU
5. Hasil deteksi serangan MITM dengan menggunakan *decision tree* adalah menggunakan *oversampling* dengan *split data training* 60% dan testing 40%, yaitu TPR 95.31%, FPR 00.01%, TNR 99.98%, FNR 04.68%, dan akurasi 97.52%.

5.2 Saran

Berdasarkan penelitian ini, maka saran untuk penelitian selanjutnya ialah sebagai berikut:

1. Penelitian selanjutnya dengan metode yang sama akan teapi diterapkan pada jenis serangan yang berbeda
2. Penelitian selanjutnya mendeteksi serangan MITM dengan secara *realtime.*
3. Penelitian selanjutnya dapat menerapkan teknik visualisasi dari deteksi serangan MITM

DAFTAR PUSTAKA

[1] A. F. S. Prisco and M. J. Freddy Duitama, "Intrusion detection system for SCADA platforms through machine learning algorithms," *2017 IEEE Colomb. Conf. Commun. Comput. COLCOM 2017 - Proc.*, pp. 1–6, 2017, doi: 10.1109/ColComCon.2017.8088210.

[2] Y. Cherdantseva *et al.*, "A review of cyber security risk assessment methods for SCADA systems," *Comput. Secur.*, vol. 56, pp. 1–27, 2016, doi: 10.1016/j.cose.2015.09.009.

[3] J. Suaboot *et al.*, "A Taxonomy of Supervised Learning for IDSs in SCADA Environments," *ACM Comput. Surv.*, vol. 53, no. 2, 2020, doi: 10.1145/3379499.

[4] Q. S. Qassim *et al.*, "Simulating command injection attacks on IEC 60870-5-104 protocol in SCADA system," *Int. J. Eng. Technol.*, vol. 7, no. 2.14 Special Issue 14, pp. 153–159, 2018, doi: 10.14419/ijet.v7i2.14.12816.

[5] M. Conti, N. Dragoni, and V. Lesyk, "A Survey of Man in the Middle Attacks," *IEEE Commun. Surv. Tutorials*, vol. 18, no. 3, pp. 2027–2051, 2016, doi: 10.1109/COMST.2016.2548426.

[6] H. Nihri, E. S. Pramukantoro, and P. H. Trisnawan, "Pengembangan IDS Berbasis J48 Untuk Mendeteksi Serangan DoS Pada Perangkat Middleware IoT," *J. Pengemb. Teknol. Inf. dan Ilmu Komput. Univ. Brawijaya*, vol. 2, no. 12, 2018.

[7] E. Hodo, S. Grebeniuk, H. Ruotsalainen, and P. Tavolato, "Anomaly detection for simulated IEC-60870-5-104 traffic," *ACM Int. Conf. Proceeding Ser.*, vol. Part F1305, 2017, doi: 10.1145/3098954.3103166.

[8] M. A. Teixeira, T. Salman, M. Zolanvari, R. Jain, N. Meskin, and M. Samaka, "SCADA system testbed for cybersecurity research using machine learning approach," *Futur. Internet*, vol. 10, no. 8, 2018, doi: 10.3390/fi10080076.

[9] D. S. Pidikiti, R. Kalluri, R. K. S. Kumar, and B. S. Bindhumadhava, "SCADA communication protocols: vulnerabilities, attacks and possible mitigations," *CSI Trans. ICT*, vol. 1, no. 2, pp. 135–141, 2013, doi: 10.1007/s40012-013-0013-5.

[10] V. Patil, V. Kulkarni, and H. Patil, "Improvised Group Key Management Protocol for SCADA System," *2018 Int. Conf. Smart City Emerg. Technol. ICSCET 2018*, pp. 1–4, 2018, doi: 10.1109/ICSCET.2018.8537287.

[11] P. Radoglou-Grammatikis, P. Sarigiannidis, I. Giannoulakis, E. Kafetzakis, and E. Panaousis, "Attacking IEC-60870-5-104 SCADA Systems," *Proc. - 2019 IEEE World Congr. Serv. Serv. 2019*, vol. 2642–939X, pp. 41–46, 2019, doi: 10.1109/SERVICES.2019.00022.

[12] J. Chromik, A. Remke, B. R. Haverkort, and G. Geist, "A Parser for Deep Packet Inspection of IEC-104: A Practical Solution for Industrial Applications," *Proc. - 49th Annu. IEEE/IFIP Int. Conf. Dependable Syst. Networks - DSN 2019 Ind. Track*, pp. 5–8, 2019, doi: 10.1109/DSN-Industry.2019.00008.

[13] P. Maynard, K. McLaughlin, and B. Haberler, "Towards Understanding Man-In-The-Middle Attacks on IEC 60870-5-104 SCADA Networks," no. January 2017, 2014, doi: 10.14236/ewic/ics-csr2014.5.

[14] M. Petr, "Description and analysis of IEC 104 Protocol Petr Matoušek," p. 38, 2017, [Online]. Available: http://www.fit.vutbr.cz/~matousp/grants.php.en?id=1101.

[15] A. Khraisat, I. Gondal, P. Vamplew, and J. Kamruzzaman, "Survey of intrusion detection systems: techniques, datasets and challenges," *Cybersecurity*, vol. 2, no. 1, 2019, doi: 10.1186/s42400-019-0038-7.

[16] V. No, E. A. Winanto, and A. Heryanto, "Visualisasi Serangan Remote to Local (R2L) Dengan Clustering K-Means," vol. 2, no. 1, pp. 359–362, 2016.

[17] O. Eigner, P. Kreimel, and P. Tavolato, “Detection of man-in-the-middle attacks on industrial control networks,” *Proc. - 2016 Int. Conf. Softw. Secur. Assur. ICSSA 2016*, pp. 64–69, 2017, doi: 10.1109/ICSSA.2016.19.

[18] B. Bhushan, G. Sahoo, and A. K. Rai, “Man-in-the-middle attack in wireless and computer networking - A review,” *Proc. - 2017 3rd Int. Conf. Adv. Comput. Commun. Autom. (Fall), ICACCA 2017*, vol. 2018-Janua, pp. 1–6, 2018, doi: 10.1109/ICACCAF.2017.8344724.

[19] W. Xie, G. Liang, Z. Dong, B. Tan, and B. Zhang, “An Improved Oversampling Algorithm Based on the Samples’ Selection Strategy for Classifying Imbalanced Data,” *Math. Probl. Eng.*, vol. 2019, 2019, doi: 10.1155/2019/3526539.

[20] N. S. Rahmi, “Ensemble-support vector machine-random undersampling: Simulation study of multiclass classification for handling high dimensional and imbalanced data,” *J. Phys. Conf. Ser.*, vol. 1613, no. 1, 2020, doi: 10.1088/1742-6596/1613/1/012064.

[21] L. Mehra, M. K. Gupta, and H. S. Gill, “An effectual & secure approach for the detection and efficient searching of Network Intrusion Detection System (NIDS),” *IEEE Int. Conf. Comput. Commun. Control. IC4 2015*, vol. 108, no. 15, pp. 37–41, 2016, doi: 10.1109/IC4.2015.7375615.

[22] S. Y. Wu and E. Yen, “Data mining-based intrusion detectors,” *Expert Syst. Appl.*, vol. 36, no. 3 PART 1, pp. 5605–5612, 2009, doi: 10.1016/j.eswa.2008.06.138.

[23] P. Maynard, K. McLaughlin, and S. Sezer, “An Open Framework for Deploying Experimental SCADA Testbed Networks,” no. 2016, pp. 92–101, 2018, doi: 10.14236/ewic/ics2018.11.

[24] B. Charbuty and A. Abdulazeez, “Classification Based on Decision Tree Algorithm for Machine Learning,” *J. Appl. Sci. Technol. Trends*, vol. 2, no. 01, pp. 20–28, 2021, doi: 10.38094/jastt20165.

SISTEM DETEKSI MAN IN THE MIDDLE (MITM) ATTACK PADA JARINGAN SUPERVISORY CONTROL AND DATA ACQUISITION (SCADA) DENGAN MENGGUNAKAN DECISION TREE

by 09011181621014 M. Rozzak Farhan

SISTEM DETEKSI MAN IN THE MIDDLE (MITM) ATTACK PADA JARINGAN SUPERVISORY CONTROL AND DATA ACQUISITION (SCADA) DENGAN MENGGUNAKAN DECISION TREE

ORIGINALITY REPORT

14%	6%	2%	13%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	Submitted to Sriwijaya University Student Paper	10%
2	Submitted to Universitas International Batam Student Paper	1%
3	Bharat Bhushan, G. Sahoo, Amit Kumar Rai. "Man-in-the-middle attack in wireless and computer networking — A review", 2017 3rd International Conference on Advances in Computing,Communication & Automation (ICACCA) (Fall), 2017 Publication	1%
4	open.library.ubc.ca Internet Source	1%
5	repository.usm.ac.id Internet Source	1%
6	comnets.ilkom.unsri.ac.id Internet Source	1%

KEMENTERIAN PENDIDIKAN, KEBUDAYAAN,
RISET DAN TEKNOLOGI
UNIVERSITAS SRIWIJAYA
FAKULTAS ILMU KOMPUTER
JURUSAN SISTEM KOMPUTER
Jalan Palembang – Prabumulih Km. 32 Indralaya Kabupaten Ogan Ilir Kode Pos 30662
Telepon (0711)7072729, 379249, 581700 Faksimili (0711) 379248, 581710
Pos-el : info@ilkom.unsri.ac.id

FORM PERBAIKAN UJIAN SKRIPSI (TUGAS AKHIR II)

Nama Mahasiswa	: M. Rozzak Farhan
NIM	: 09011181621014.
Jurusan	: Sistem Komputer
Hari / Tanggal	: Kamis / 2 Desember 2021
Waktu	: 10:00 s.d 10:30 WIB
Judul Tugas Akhir	: Sistem Deteksi Man In The Middle (MITM) Attack pada Jaringan Supervisory Control and Data Acquisition (SCADA) dengan menggunakan Decision Tree
Pembimbing	: Deris Stiawan, M.T., Ph.D Ahmad Heryanto, M.T
Perbaikan/Saran	:

Jangka Waktu Perbaikan :

Telah diperbaiki sesuai dengan saran dan koreksi tim penguji ujian komprehensif.

No.	Nama Penguji	Status Penguji	Tanda Tangan
1.	Deris Stiawan, M.T., Ph.D	Pendamping (Pembela) I	

Palembang, ~~2~~ 30 Desember 2021
Ketua Jurusan Sistem Komputer

Dr. Ir. H. Sukemi, M.T.
NIP 196612032006041001

KEMENTERIAN PENDIDIKAN, KEBUDAYAAN,
RISET DAN TEKNOLOGI
UNIVERSITAS SRIWIJAYA
FAKULTAS ILMU KOMPUTER
JURUSAN SISTEM KOMPUTER
Jalan Palembang – Prabumulih Km. 32 Indralaya Kabupaten Ogan Ilir Kode Pos 30662
Telepon (0711)7072729, 379249, 581700 Faksimili (0711) 379248, 581710
Pos-el : info@ilkom.unsri.ac.id

FORM PERBAIKAN UJIAN SKRIPSI (TUGAS AKHIR II)

Nama Mahasiswa	: M. Rozzak Farhan
NIM	: 09011181621014.
Jurusan	: Sistem Komputer
Hari / Tanggal	: Kamis / 2 Desember 2021
Waktu	: 10:00 s.d 10:30 WIB
Judul Tugas Akhir	: Sistem Deteksi Man In The Middle (MITM) Attack pada Jaringan Supervisory Control and Data Acquisition (SCADA) dengan menggunakan Decision Tree
Pembimbing	: Deris Stiawan, M.T., Ph.D Ahmad Heryanto, M.T
Perbaikan/Saran	:

Jangka Waktu Perbaikan :

Telah diperbaiki sesuai dengan saran dan koreksi tim penguji ujian komprehensif.

No.	Nama Penguji	Status Penguji	Tanda Tangan
1.	Ahmad Heryanto, M.T	Pendamping (Pembela) II	

Palembang, 30 Desember 2021
Ketua Jurusan Sistem Komputer

Dr. Ir. H. Sukemi, M.T.
NIP 196612032006041001

KEMENTERIAN PENDIDIKAN, KEBUDAYAAN,
RISET DAN TEKNOLOGI
UNIVERSITAS SRIWIJAYA
FAKULTAS ILMU KOMPUTER
JURUSAN SISTEM KOMPUTER
Jalan Palembang – Prabumulih Km. 32 Indralaya Kabupaten Ogan Ilir Kode Pos 30662
Telepon (0711)7072729, 379249, 581700 Faksimili (0711) 379248, 581710
Pos-el : info@ilkom.unsri.ac.id

FORM PERBAIKAN UJIAN SKRIPSI (TUGAS AKHIR II)

Nama Mahasiswa	: M. Rozzak Farhan
NIM	: 09011181621014.
Jurusan	: Sistem Komputer
Hari / Tanggal	: Kamis / 2 Desember 2021
Waktu	: 10:00 s.d 10:30 WIB
Judul Tugas Akhir	: Sistem Deteksi Man In The Middle (MITM) Attack pada Jaringan Supervisory Control and Data Acquisition (SCADA) dengan menggunakan Decision Tree
Pembimbing	: Deris Stiawan, M.T., Ph.D Ahmad Heryanto, M.T
Perbaikan/Saran	:

* 4.10 Implementasi Decision Tree
* Tambah Data Paket Serangan

Jangka Waktu Perbaikan :

Telah diperbaiki sesuai dengan saran dan koreksi tim penguji ujian komprehensif.

No.	Nama Penguji	Status Penguji	Tanda Tangan
1.	Huda Ubaya, M.T	Penguji	

Palembang, 30 Desember 2021
Ketua Jurusan Sistem Komputer

Dr. Ir. H. Sukemi, M.T.
NIP 196612032006041001