

**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 :

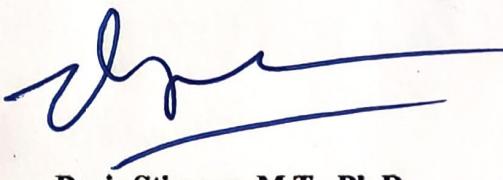
M. Rozzak Farhan  
09011181621014

Indralaya, Desember 2021

Mengetahui,

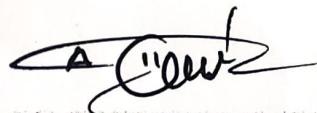
Pembimbing Tugas Akhir I

Pembimbing Tugas Akhir II



Deris Stiawan, M.T., Ph.D

NIP. 197806172006041002



Ahmad Heryanto, S.Kom., M.T.

NIP. 198701222015041002

Ketua Jurusan Sistem Komputer *20/1/22*



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

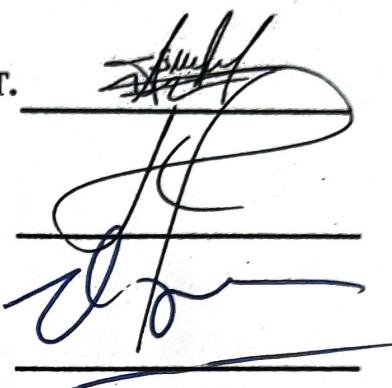
## **HALAMAN PERSETUJUAN**

Telah diuji dan lulus pada :

Hari : Kamis  
Tanggal : 2 Desember 2021

**Tim Pengaji :**

**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 (Pariantto) 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 kehadiran 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

	<b>Halaman</b>
<b>HALAMAN JUDUL .....</b>	i
<b>HALAMAN PENGESAHAN.....</b>	ii
<b>HALAMAN PERSETUJUAN .....</b>	iii
<b>HALAMAN PERNYATAAN.....</b>	iv
<b>HALAM PERSEMBAHAN .....</b>	v
<b>KATA PENGATAR.....</b>	vi
<b>ABSTRACTION .....</b>	viii
<b>ABSTRAK .....</b>	ix
<b>DAFTAR ISI.....</b>	x
<b>DAFTAR GAMBAR.....</b>	xiii
<b>DAFTAR TABEL .....</b>	xv
<b>DAFTAR RUMUS .....</b>	xvi
<b>BAB I</b>	
<b>PENDAHULUAN</b>	
1.1 Latar Belakang .....	1
1.2 Tujuan .....	2
1.3 Manfaat .....	3
1.4 Rumusan Masalah.....	3
1.5 Batasan Masalah .....	3
1.6 Metodologi Penelitian.....	3
1.7 Sistematika Penulisan .....	4
<b>BAB II</b>	
<b>TINJAUAN PUSTAKA</b>	

2.1	Diagram Konsep Penelitian .....	6
2.2	Supervisory Control and Data Acquisition (SCADA).....	6
2.3	Protocol IEC-60870-5-104 / IEC-104.....	7
2.3.1	Application Service Data Unit (ASDU) .....	8
2.3.2	Application Protocol Control Information (APCI) .....	9
2.4	Intrusion Detection System (IDS).....	9
2.5	Klasifikasi IDS.....	10
2.5.1	Klasifikasi IDS Sumber Data ( <i>Data Resource</i> ) .....	10
2.5.2	Klasifikasi IDS Metode Deteksi IDS .....	10
2.6	Man in The Middle (MITM).....	11
2.6.1	Jenis MITM.....	11
2.6.1.1	Spoofing Based MITM Attack .....	11
2.6.1.2	TSL/SSL MITM Attack.....	12
2.6.1.3	BGP (Border Gateway Protocol) Based MITM Attack.....	12
2.6.1.4	FBS (False Base Station) Based MITM Attack.....	12
2.7	<i>Synthetic Minority Oversampling Technique</i> (SMOTE) .....	13
2.8	<i>Random Under Sampling</i> .....	13
2.9	Algoritma <i>Decision Tree</i> .....	14
2.10	Evaluasi Performa Metode <i>Decision Tree</i> .....	15

### **BAB III**

#### **METODOLOGI PENELITIAN**

3.1	Pendahuluan.....	16
3.2	Kerangka Kerja Penelitian.....	16
3.3	Perancangan Sistem.....	17
3.3.1	Perangkat Penelitian.....	18
3.4	Dataset <i>Testbed</i> .....	18

3.5 Deteksi serangan dengan Menggunakan Snort IDS .....	19
3.6 Data Filtering .....	20
3.7 Data Extraction.....	20
3.8 Mencari Pola Serangan Man In The Middle .....	22
3.9 <i>Decision Tree</i> .....	23

## **BAB IV**

### **HASIL DAN ANALISIS**

4.1 Pendahuluan.....	25
4.2 <i>Raw Dataset</i> .....	25
4.3 Serangan MITM.....	25
4.4 <i>Snort</i> sebagai IDS .....	26
4.5 Ekstraksi Dataset.....	27
4.6 Pengenalan Pola Serangan.....	27
4.7 Hasil Data Ekstraksi .....	29
4.8 <i>Oversampling Dataset</i> .....	31
4.9 <i>Undersampling Dataset</i> .....	32
4.10 Decision Tree .....	33
4.11 Perhitungan Confusion Matrix.....	33

## **BAB V**

### **KESIMPULAN**

5.1 Kesimpulan .....	43
5.2 Saran .....	43

<b>DAFTAR PUSTAKA</b> .....	44
-----------------------------	----

## DAFTAR GAMBAR

	<b>Halaman</b>
<b>Gambar 2.1</b> Diagram Konsep Penelitian .....	6
<b>Gambar 2.2</b> SCADA Arsitektur .....	7
<b>Gambar 2.3</b> <i>Payload</i> Paket IEC 60870- 5-104 / APDU .....	8
<b>Gambar 2.4</b> ASDU Format.....	8
<b>Gambar 2.5</b> APCI Format.....	9
<b>Gambar 2.6</b> Arsitektur Dasar IDS .....	9
<b>Gambar 2.7</b> Struktur <i>Decision Tree</i> .....	14
<b>Gambar 3.1</b> Kerangka Kerja .....	17
<b>Gambar 3.2</b> <i>Flowchart Extraction</i> .....	20
<b>Gambar 3.3</b> <i>Flowchart Snort</i> IDS .....	22
<b>Gambar 3.4</b> Hubungan <i>raw data</i> , <i>snort alert</i> , dan data ekstraksi .....	23
<b>Gambar 3.5</b> <i>Flowchart</i> Program Decision Tree .....	24
<b>Gambar 4.1</b> Dataset pcap.....	25
<b>Gambar 4.2</b> <i>Log Alert Snort</i> IDS .....	26
<b>Gambar 4.3</b> Dataset CSV.....	27
<b>Gambar 4.4</b> Paket Normal IEC 104.....	27
<b>Gambar 4.5</b> Paket Serangan MITM IEC 104 .....	28
<b>Gambar 4.6</b> IEC 104 ASDU <i>Types</i> .....	29
<b>Gambar 4.7</b> Perbandingan Hasil Ekstraksi Data IEC IEC 104 Normal .....	30
<b>Gambar 4.8</b> Perbandingan Hasil Ekstraksi Data IECIEC 104 Serangan.....	30
<b>Gambar 4.9</b> Data Sebelum SMOTE .....	31
<b>Gambar 4.10</b> Data Setelah SMOTE .....	32

<b>Gambar 4.11</b> Data Sebelum RUS .....	32
<b>Gambar 4.12</b> Data Setelah RUS .....	33
<b>Gambar 4.13</b> Decision Tree Code .....	33
<b>Gambar 4.14</b> <i>Confusion Matrix Oversampling Training 80%</i> .....	34
<b>Gambar 4.15</b> <i>Confusion Matrix Undersampling Training 80%</i> .....	34
<b>Gambar 4.16</b> <i>Confusion Matrix Oversampling Testing 20%</i> .....	35
<b>Gambar 4.17</b> <i>Confusion Matrix Undersampling Testing 20%</i> .....	35
<b>Gambar 4.18</b> <i>Confusion Matrix Oversampling Training 70%</i> .....	36
<b>Gambar 4.19</b> <i>Confusion Matrix Undersampling Training 70%</i> .....	36
<b>Gambar 4.20</b> <i>Confusion Matrix Oversampling Testing 30%</i> .....	37
<b>Gambar 4.21</b> <i>Confusion Matrix Undersampling Testing 30%</i> .....	37
<b>Gambar 4.22</b> <i>Confusion Matrix Oversampling Training 60%</i> .....	38
<b>Gambar 4.23</b> <i>Confusion Matrix Undersampling Training 60%</i> .....	38
<b>Gambar 4.24</b> <i>Confusion Matrix Oversampling Testing 40%</i> .....	39
<b>Gambar 4.25</b> <i>Confusion Matrix Undersampling Testing 40%</i> .....	39
<b>Gambar 4.26</b> Grafik hasil dengan <i>Oversampling</i> .....	40
<b>Gambar 4.27</b> Grafik hasil dengan <i>Undersampling</i> .....	41

## DAFTAR TABEL

	<b>Halaman</b>
<b>Tabel 1</b> Confusion Matrix .....	15
<b>Tabel 2</b> Alert Confusion Matrix .....	15
<b>Tabel 3</b> Perangkat Penelitian .....	19
<b>Tabel 4</b> Atribut Extraction Protocol IEC 104.....	22
<b>Tabel 5</b> <i>Rules Snort</i> .....	26
<b>Tabel 6</b> Hasil dengan <i>Oversampling</i> .....	40
<b>Tabel 7</b> Hasil dengan <i>Undersampling</i> .....	41
<b>Tabel 8</b> Hasil Terbaik .....	42

## DAFTAR RUMUS

	<b>Halaman</b>
<b>Rumus 1</b> <i>Accuracy</i> .....	15
<b>Rumus 2</b> <i>TruePositif Rate</i> .....	15
<b>Rumus 3</b> <i>False Positif Rate</i> .....	15
<b>Rumus 4</b> <i>True Negatife Rate</i> .....	15
<b>Rumus 5</b> <i>False Negatif Rate</i> .....	15
<b>Rumus 6</b> <i>Precision</i> .....	15

# 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 menggunakan 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 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) dengan 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 keakurasaian 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 jaringan 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.

## 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. Havercort, 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.