

**VISUALISASI SERANGAN *MAN IN THE MIDDLE* (MITM)  
PADA JARINGAN *SUPERVISORY CONTROL AND DATA  
ACQUISITION* (SCADA) MENGGUNAKAN SUPPORT  
VECTOR MACHINE**

**TUGAS AKHIR**

**Diajukan Untuk Melengkapi Salah Satu Syarat  
Memperoleh Gelar Sarjana Komputer**



**Oleh :**

**Harry Anugrah  
09011181621116**

**JURUSAN SISTEM KOMPUTER  
FAKULTAS ILMU KOMPUTER  
UNIVERSITAS SRIWIJAYA  
2021**

**UNIVERSITAS SRIWIJAYA 2021**

**LEMBAR PENGESAHAN**

**VISUALISASI SERANGAN *MAN IN THE MIDDLE* (MITM)  
PADA JARINGAN *SUPERVISORY CONTROL AND DATA  
ACQUISITION* (SCADA) MENGGUNAKAN SUPPORT  
VECTOR MACHINE**

**TUGAS AKHIR**

Diajukan Untuk Melengkapi Salah Satu Syarat  
Memperoleh Gelar Sarjana Komputer

Oleh :

**HARRY ANUGRAH  
09011181621116**

Indralaya, 27 Mei 2021

Mengetahui,

Pembimbing Tugas Akhir I



Deris Stiawan, M.T., Ph.D.  
NIP. 197806172006041002

Pembimbing Tugas Akhir II



Ahmad Heryanto, S.Kom., M.T.  
NIP. 198701222015041002

Ketua Jurusan Sistem Komputer



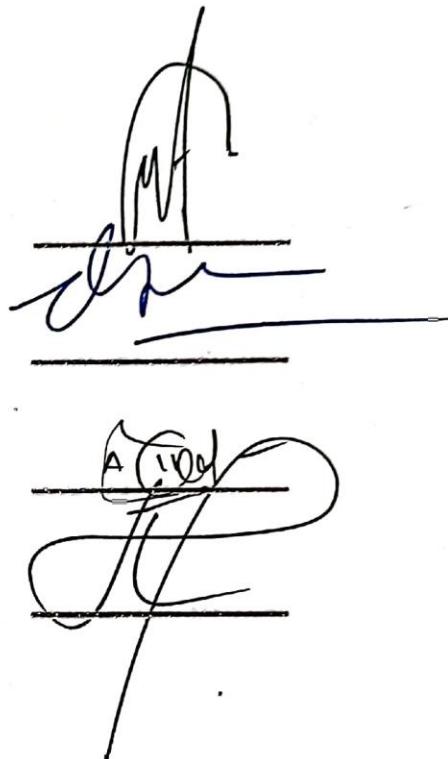
## HALAMAN PERSETUJUAN

Telah diuji dan lulus pada:

Hari : Rabu  
Tanggal : 10 Maret 2021

Tim Penguji:

1. Ketua : Ahmad Zarkasi, M.T
2. Sekretaris I : Deris Stiawan, M.T., Ph.D
3. Sekretaris II : Ahmad Heryanto, S.Kom., M.T.
4. Anggota I : Huda Ubaya, M.T'



Mengetahui,

Ketua Jurusan Sistem Komputer



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

## **LEMBAR PERNYATAAN**

Yang bertanda tangan dibawah ini:

Nama : Harry Anugrah  
NIM : 09011181621116  
Judul : Visualisasi Serangan Man in The Middle (MITM) Pada Jaringan Supervisory Control and Data Acquisition (SCADA) Menggunakan Support Vector Machine

Hasil Pengecekan Software Turnitin : 15%

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, 27 Mei 2021



Harry Anugrah

**NIM. 09011181621116**

## **HALAMAN PERSEMBAHAN**

“Skripsi ini dikerjakan sebelum dan sesudah Ayah pergi, 25 Agustus 2020.”

**“Maaf yo Ayah baru selesai”**

Skripsi ini saya persembahkan khusus untuk :

- Almarhum Ayah (Cik Hasan, S.E) dan Mamak (Ratna Zulaillah) tercinta yang tak pernah berhenti memanjatkan do'a, memotivasi, mendidik dan mengorbankan segala hal kepada putranya demi menggapai cita-cita yang diinginkan
- Seluruh keluarga yang berperan, membantu dan ikut andil dalam perjalananku menuju kesuksesan
- Teman-teman satu grup riset yang selalu menjadi tempat berdiskusi dan bertanya dikala susah, dan
- Dosen pembimbing terbaik yang pernah ada, Bapak Deris Stiawan M.T., Ph.D. dan Bapak Ahmad Heryanto S.Kom., M.T.

Terimakasih banyak...

## KATA PENGANTAR

Puji dan syukur kepada Allah SWT, atas limpahan rahmat dan karunia-Nya yang telah memberikan penulis kesehatan dan kesempatan sebaik-baiknya, sehingga penulis dapat merampungkan Proposal Tugas Akhir ini dengan judul “Visualisasi Serangan *Man In The Middle* (MITM) pada jaringan *Supervisory Control And Data Acquisition* (SCADA) Menggunakan *Support Vector Machine*”.

Penulisan Proposal Tugas Akhir ini dilakukan untuk melengkapi salah satu syarat memperoleh gelar Sarjana Komputer di Jurusan Sistem Komputer Fakultas Ilmu Komputer Universitas Sriwijaya. Pada kesempatan ini juga, penulis menyampaikan ucapan terima kasih yang sebesar-besarnya kepada semua pihak yang telah membantu baik dari segi moril maupun 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. Ayah Cik Hasan dan Mamak Ratna Zulaillah serta keluarga penulis tercinta, yang telah mencerahkan segenap cinta dan kasih sayang serta perhatian moril maupun materil kepada penulis selama melaksanakan dan mengikuti perkuliahan di Jurusan Sistem Komputer Fakultas Ilmu Komputer Universitas Sriwijaya, semoga Allah SWT selalu melindungi, melimpahkan rahmat, kesehatan, karunia dan keberkahan di dunia maupun di akhirat atas budi baik yang telah diberikan kepada penulis.
2. Bapak Jaidan Jauhari, S.Pd., M.T., selaku Dekan Fakultas Ilmu Komputer Universitas Sriwijaya.
3. Bapak Dr. Ir. H. Sukemi, M.T., selaku Ketua Jurusan Sistem Komputer Fakultas Ilmu Komputer Universitas Sriwijaya.

4. Bapak Dr. Reza Firsandaya Malik, 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 I 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 Renny Virgasari 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 angkatan 2016, Terutama Pasukan SCADA, Terutama Yogi Yaspranika dan Sergio Septiano serta Teman-Teman Sistem Komputer Fakultas Ilmu Komputer Universitas Sriwijaya.
10. Almamaterku, Komputerku Xiti, Laptop lama Bambank, Laptop pengganti untuk tugas akhir Yosop, dan motor yang selalu menemani kuliahku Yosep.

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 Proposal Tugas Akhir ini dan semoga bermanfaat bagi kita semua baik dalam dunia Pendidikan maupun dalam lingkungan masyarakat. Aamiin.

Indralaya, 27 Mei 2021  
Penulis

Harry Anugrah  
NIM. 09011181621116

# **VISUALISASI SERANGAN MAN IN THE MIDDLE (MITM) PADA JARINGAN SUPERVISORY CONTROL AND DATA ACQUISITION (SCADA) MENGGUNAKAN SUPPORT VECTOR MACHINE**

Harry Anugrah (09011181621116)

Jurusan Sistem Komputer, Fakultas Ilmu Komputer

Universitas Sriwijaya

E-mail : [herryanugrah98@gmail.com](mailto:herryanugrah98@gmail.com)

## **ABSTRAK**

*Supervisory Control And Data Acquisition* adalah *Industry Control System* otomatis yang digunakan untuk memonitoring dan mengendalikan proses di sektor industri dan sektor infrastruktur *Critical* nasional. Salah satu protocol komunikasi SCADA adalah IEC 60870-5-104 yang dimana digunakan untuk mengirim pesan. Serangan MITM adalah sebuah proses serangan dimana *hacker* menyelinap di tengah-tengah sebuah koneksi untuk mendapatkan informasi tanpa diketahui, memodifikasi, memotong koneksi dan bahkan dapat mencuri data yang sangat penting. Pada penelitian ini *Support Vector Machine* digunakan untuk membedakan paket normal dan paket serangan. Hasil deteksi dievaluasi dengan *Confusion Matrix* untuk menentukan akurasi deteksi serangan MITM dengan metode SVM. Dari hasil penelitian ini, akurasi yang didapat adalah 97,78%. Visualisasi pada penelitian ini bertujuan untuk mempermudah dalam mengenali dan menyimpulkan perbedaan dari paket data normal dan paket data serangan. Indikator yang digunakan untuk perbandingan adalah *frame\_length* dan *causeTx*.

**Kata Kunci :** *Supervisory Control And Data Acquisiton, Man In The Middle, Intrusion Detection System, Support Vector Machine, Confusion Matrix.*

**Mengetahui,**

**Pembimbing I Tugas Akhir**



**Deris Stiawan, M.T., Ph.D.**

NIP. 197806172006041002

**Pembimbing II Tugas Akhir**



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

NIP. 198701222015041002



**MAN IN THE MIDDLE (MITM) ATTACK VISUALIZATION ON  
SUPERVISORY CONTROL AND DATA ACQUISITION (SCADA)  
NETWORK USING SUPPORT VECTOR MACHINE**

Harry Anugrah (09011181621116)

Dept. of Computer Engineering, Faculty of Computer Science,  
Sriwijaya University

E-mail : herryanugrah98@gmail.com

**ABSTRACT**

Supervisory Control And Data Acquisition is an Industry Control System used to monitor and control processes in the critical national infrastructure sector, one of the communication protocols SCADA is IEC 60870-5-104 which is used to send messages. The MITM attack was a process of attacks in which hackers slipped in the middle of a connection to obtain unknown information, modify, cut connections and can even steal very important data. On this research, Support Vector Machine is used to distinguish between normal packages and packages Attack. Detection results evaluated with Confusion Matrix to determine accuracy mitm attack detection with SVM method. From the results of this research, the accuracy obtained is 97.78%. The Visualization in this Research aims to make it easier for in recognizing and infering differences from normal data packets and data Attack. Indicators used for comparison are frame\_length and causeTx.

**Keyword:** Supervisory Control And Data Acquisiton, Man In The Middle, Intrusion  
Detection System Suport Vector Machine, Confusion Matrix.

Mengetahui,

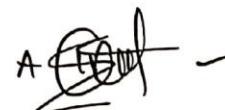
Pembimbing I Tugas Akhir



Deris Stiawan, M.T., Ph.D.

NIP. 197806172006041002

Pembimbing II Tugas Akhir



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

NIP. 198701222015041002

Ketua Jurusan Sistem Komputer



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

NIP. 196612032006041

## DAFTAR ISI

<b>HALAMAN JUDUL .....</b>	<b>i</b>
<b>HALAMAN PENGESAHAN .....</b>	<b>ii</b>
<b>HALAMAN PERSETUJUAN .....</b>	<b>iii</b>
<b>HALAMAN PERNYATAAN.....</b>	<b>iv</b>
<b>HALAMAN PERSEMBAHAN .....</b>	<b>v</b>
<b>KATA PENGANTAR .....</b>	<b>vi</b>
<b>ABSTRAK .....</b>	<b>vii</b>
<b>ABSTRACT .....</b>	<b>viii</b>
<b>DAFTAR ISI .....</b>	<b>ix</b>
<b>DAFTAR GAMBAR .....</b>	<b>xii</b>
<b>DAFTAR TABEL .....</b>	<b>xiv</b>
<b>DAFTAR RUMUS .....</b>	<b>xv</b>

### **BAB I**

#### **PENDAHULUAN**

1.1. Latar Belakang.....	1
1.2. Tujuan .....	3
1.3. Manfaat .....	3
1.4. Rumusan Masalah .....	3
1.5. Batasan Masalah .....	4
1.6. Metodologi Penelitian .....	4
1.7. Sistematika Penulisan .....	5

### **BAB II**

#### **TINJAUAN PUSTAKA**

2.1. Diagram Konsep Penelitian .....	6
2.2. <i>Supervisory Control And Data Acquisition .....</i>	7

2.2.1.	Protocol IEC 60870-5-104 .....	8
2.2.2.	APCI Format .....	9
2.2.3.	ASDU Format .....	10
2.3.	<i>Man In The Middle</i> .....	11
2.3.1.	Tipe <i>Man In The Middle</i> .....	12
2.4.	TCP/IP SCADA.....	13
2.5.	<i>Intrusion Detection System</i> .....	13
2.6.	Klasifikasi IDS Berdasarkan Penempatan <i>Deployment</i> .....	15
2.7.	Klasifikasi IDS Berdasarkan Metode Deteksi .....	15
2.8.	Metode Penelitian Umum IDS .....	16
2.9.	<i>Support VectorMachine</i> ... .....	17
2.10	Evaluasi Performa Metode <i>Support Vector Machine</i> .....	17
2.11.	<i>Synthetic Minority Oversampling Technique</i> .....	19
2.12.	Dataset.....	19

### BAB III

#### METODOLOGI PENELITIAN

3.1.	Pendahuluan.....	21
3.2.	Kerangka Kerja Penelitian .....	21
3.3.	Perancangan System.....	23
3.3.1.	Kebutuhan Perangkat Lunak .....	23
3.4.	<i>Data Exploration dan Preparation</i> .....	23
3.5.	Data Ekstraksi.....	24
3.6.	Deteksi Serangan Menggunakan <i>Snort IDS</i> .....	27
3.7.	Mencari Pola Serangan <i>Man In The Middle</i> .....	29
3.8.	<i>SMOTE</i> .....	30
3.9.	<i>Support Vector Machine</i> .....	30
3.8.	Program Deteksi dengan <i>Support Vector Machine</i> .....	32

## **BAB IV**

### **HASIL DAN ANALISIS**

4.1. Pendahuluan .....	33
4.2. Analisis Dataset .....	33
4.3. Pengenalan Pola Serangan <i>Man In The Middle</i> .....	34
4.4. Hasil Data Ekstraksi .....	36
4.5. Hasil Visualisasi.....	39
4.5.1. Grafik Data Normal .....	39
4.5.2. Grafik Data Serangan.....	42
4.6. Penerapan Deteksi MITM menggunakan SVM.....	44
4.6.1. <i>Missing Value</i> .....	44
4.6.2. <i>Oversampling</i> .....	44
4.7. Evaluasi <i>Confusion Matrix</i> .....	46

## **BAB V**

### **KESIMPULAN DAN SARAN**

5.1. Kesimpulan .....	49
5.2. Saran.....	50
Daftar Pustaka.....	51

## DAFTAR GAMBAR

Halaman

<b>Gambar 2.1.</b> Diagram Konsep Penelitian .....	6
<b>Gambar 2.2.</b> Arsitektur <i>Scada</i> .....	7
<b>Gambar 2.3.</b> Format Frame tipe I.....	8
<b>Gambar 2.4.</b> Frame APCI dan APDU.....	9
<b>Gambar 2.5.</b> Format APCI.....	10
<b>Gambar 2.6.</b> Format ASDU.....	10
<b>Gambar 2.7.</b> Model Skema Serangan MITM .....	11
<b>Gambar 2.8.</b> Model Skema Serangan MITM pada SCADA.....	11
<b>Gambar 2.9.</b> Metode dan Teknik IDS.....	14
<b>Gambar 2.10.</b> Struktur IDS .....	14
<b>Gambar 2.11.</b> Diagram Metode Penelitian Umum IDS.....	16
<b>Gambar 2.12.</b> <i>Support Vector Machine</i> .....	17
<b>Gambar 2.13.</b> Diagram <i>Network sample testbed</i> .....	19
<b>Gambar 3.1.</b> Kerangka Kerja Penelitian .....	22
<b>Gambar 3.2.</b> Flowchart Data Ekstraksi.....	24
<b>Gambar 3.3.</b> <i>CauseTx</i> .....	25
<b>Gambar 3.4.</b> Flowchart Snort IDS .....	27
<b>Gambar 3.5.</b> SID Snort.....	28
<b>Gambar 3.6.</b> Hubungan antara <i>alert snort</i> , <i>raw data</i> dan <i>data ekstraksi</i> .....	29
<b>Gambar 3.7.</b> Flowchart SVM .....	31
<b>Gambar 4.1.</b> Dataset Pcap .....	33
<b>Gambar 4.2.</b> Paket Normal IEC 104 .....	34
<b>Gambar 4.3.</b> Paket Serangan IEC 104 .....	35
<b>Gambar 4.4.</b> Validasi data ekstraksi IEC 104 Normal.....	37

<b>Gambar 4.5.</b> Validasi data ekstraksi IEC 104 Serangan.....	38
<b>Gambar 4.6.</b> Ekstraksi Data Normal .....	39
<b>Gambar 4.7.</b> Grafik <i>Frame</i> Data Normal.....	40
<b>Gambar 4.8.</b> Grafik <i>Frame_length</i> Data Normal .....	40
<b>Gambar 4.9.</b> Grafik <i>causeTx</i> Data Normal.....	41
<b>Gambar 4.10.</b> Ekstraksi Data Serangan.....	42
<b>Gambar 4.11.</b> Grafik <i>Frame</i> Data Serangan .....	42
<b>Gambar 4.12.</b> Grafik <i>Frame_length</i> Serangan .....	43
<b>Gambar 4.13.</b> Grafik <i>causeTx</i> Serangan .....	43
<b>Gambar 4.14.</b> Grafik Data Normal dan Serangan <i>Original</i> .....	45
<b>Gambar 4.15.</b> Grafik Data Normal dan Serangan SMOTE.....	45
<b>Gambar 4.16.</b> <i>Confusion Matrix SVM</i> .....	46
<b>Gambar 4.17.</b> <i>Confusion Matrix SVM + SMOTE</i> .....	47

## DAFTAR TABEL

	Halaman
<b>TABEL 1.</b> Komunikasi TCP/IP SCADA .....	13
<b>TABEL 2.</b> Parameter Confusion Matrix .....	18
<b>TABEL 3.</b> Kebutuhan Perangkat Lunak .....	23
<b>TABEL 4.</b> Atribut Data Ekstraksi.....	25
<b>TABEL 5.</b> Hasil <i>Accuracy</i> , <i>Detection Rate</i> , <i>False Alert rate</i> dan <i>Precision</i> .....	48

## DAFTAR RUMUS

Halaman

<b>Rumus 1.</b> <i>Accuracy</i> .....	18
<b>Rumus 2.</b> <i>True Positif Rate</i> .....	18
<b>Rumus 3.</b> <i>False Positif Rate</i> .....	18
<b>Rumus 4.</b> <i>True Negatife Rate</i> .....	18
<b>Rumus 5.</b> <i>False Negatif Rate</i> .....	18
<b>Rumus 6.</b> <i>Precisiom</i> .....	18

## BAB I

### PENDAHULUAN

#### 1.1. Latar Belakang

*Supervisory Control And Data Acquisition* (SCADA) adalah *Industry Control System* (ICS) otomatis yang digunakan untuk memonitoring dan mengendalikan proses di sektor industri dan sektor infrastruktur *Critical* nasional[1]. Seperti pembangkit dan distribusi energi dan jaringan tenaga listrik. Secara historis[2] system SCADA dirancang dengan jaringan *private network*, namun karena penyebaran perangkat SCADA secara geografis, sekarang komunikasi SCADA menggunakan internet.

Salah satu protocol komunikasi SCADA adalah IEC 60870-5-104 atau dikenal juga sebagai IEC104 yang dimana digunakan untuk mengirim pesan telekontrol dasar antar perangkat berdasarkan standar TCP/IP, yang memungkinkan transmisi data secara simultan antara beberapa perangkat dan layanan[3]. Protocol IEC104 memiliki kerentanan pada keamanan *application layer* dan *data link layer*. Kerentanan pada *application layer* menyebabkan protocol ini dapat diserang dengan *spoofing*. Pada *data link layer* menyebabkan protocol ini dapat di serang menggunakan *snipping*, *modification data* dan *replay attack*[4].

Terdapat banyak serangan *cyber* yang bisa terjadi di system SCADA, salah satu nya serangan *Man In The Middle* (MITM) [5] yang mempunyai risiko sangat tinggi bagi jaringan SCADA. Serangan MITM adalah sebuah proses serangan dimana *hacker* menyelinap di tengah-tengah sebuah koneksi untuk mendapatkan informasi tanpa diketahui, memodifikasi, memotong koneksi dan bahkan dapat mencuri data yang sangat penting [6].

Ada pendekatan yang dapat digunakan untuk mencegah hal tersebut yaitu menggunakan *Intrusion Detection System* (IDS). IDS merupakan system yang sangat penting dalam keamanan jaringan, dimana IDS berfungsi untuk mendeteksi kemungkinan adanya serangan oleh *attacker*. Beberapa penelitian [7] menggunakan pendekatan (IDS) telah dilakukan pada system SCADA, seperti *signature-based* dan *anomaly-based*. System IDS diperlukan untuk memonitor dan

mendeteksi ancaman terhadap sistem akibat penyalahgunaan oleh pengguna asli maupun serangan yang disengaja oleh *hacker*[8].

Beberapa penelitian [7] menggunakan pendekatan (IDS) telah dilakukan pada system SCADA, seperti *signature-based* dan *anomali-based*. System IDS diperlukan untuk memonitor dan mendeteksi ancaman terhadap system akibat penyalahgunaan oleh pengguna asli maupun serangan yang disengaja oleh *hacker*[8].

Pada penelitian [9] membahas permasalahan bagaimana meningkatkan *performance* IDS dengan memproses data *alert* melalui tiga tahapan, tahapan persiapan, tahapan *clustering* dan tahapan visualisasi. Sedangkan pada penelitian yang lain [10] membahas bagaimana memvisualisasikan *file log* dengan beberapa metode perancangan visualisasi untuk meningkatkan efektifitas pada system analisis keamanan seperti *text-based analysis*, *parallel visualization methods*, *hierarchical visualization method* dan *three-dimensional visualization*.

Pada penelitian [7] membahas penerapan *rule-based* IDS untuk jaringan SCADA protocol IEC104 menggunakan analisis protocol dan metode *Deep Packet Inspection*. Hasil penelitian ini menunjukkan *rule-based IDS* efektif dalam mengidentifikasi semua paket serangan tanpa ada *false alert* untuk serangan yang terdapat pada database system.

Pada penelitian [11] membahas tentang system deteksi anomali berbasis model-based untuk serangan pada gardu daya listrik berdasarkan protocol IEC104, menggunakan tiga model serangan yaitu, *Arp Spoofing*, *DoS* dan *Command Injection*. Model deteksi dirancang dengan algoritma *Supervised Learning* , dari hasil pengujian didapat bahwa algoritma *Rule Learners* memiliki akurasi terbaik yaitu 91,69%. Sedangkan pada penelitian lainnya [12] menunjukkan hasil deteksi anomali dengan algoritma *Support Vector Machine* mempunyai akurasi yaitu 99,6%.

Berdasarkan hal tersebut, maka penelitian tugas akhir akan merancang *Intrusion Detection System* untuk mendeteksi serangan *Man In The Middle* di jaringan *Supervisory Control and data Acquisition* protocol IEC 60870-5-104 dengan metode *Support Vector Machine*.

## 1.2. Tujuan

Adapun tujuan dari penelitian Tugas Akhir ini adalah sebagai berikut :

1. Membedakan antara trafik normal dan trafik serangan pada jaringan *Supervisory Control And Data Acquisition* sehingga dapat mendeteksi serangan *Man In The Middle*.
2. Menerapkan algoritma *Support Vector Machine* untuk deteksi trafik serangan *Man In The Middle* pada jaringan *Supervisory Control And Data Acquisition*
3. Memvisualisasi data normal dan serangan *Man In The Middle* dalam bentuk grafik.
4. Menganalisa Keakurasi Metode *Support Vector Machine* untuk mendeteksi serangan *Man In The Middle* pada jaringan *Supervisory Control And Data Acquisition*.

## 1.3. Manfaat

Adapun manfaat dari penelitian Tugas Akhir ini adalah sebagai berikut :

1. Dapat membedakan trafik serangan dan trafik normal pada jaringan *Supervisory Control And Data Acquisition*
2. Dapat mendeteksi serangan *Man in The Middle* pada jaringan *Supervisory Control And Data Acquisition*
3. Dapat mengetahui tingkat akurasi metode *Support Vector Machine* dalam deteksi serangan *Man in The Middle* pada jaringan *Supervisory Control And Data Acquisition*.

## 1.4. Rumusan Masalah

Adapun rumusan masalah dalam penelitian Tugas Akhir ini adalah sebagai berikut:

1. Bagaimana cara mengekstrak dataset, kemudian mencari pola serangan *Man In The Middle*.
2. Bagaimana metode *Support Vector Machine* dapat mengenali serangan *Man in The Middle* pada jaringan *Supervisory Control And Data Acquisition* pada dataset.

3. Bagaimana memvisualisasikan pola serangan *Man In The Middle* kedalam bentuk grafis.

### **1.5. Batasan Masalah**

Berikut adalah batasan masalah dalam penelitian Tugas Akhir ini:

1. Pengujian dilakukan pada jaringan *Supervisory Control And Data Acquisition* protocol IEC 60870-5-104.
2. Mengklasifikasi serangan *Man In The Middle* pada jaringan *Supervisory Control And Data Acquisition* menggunakan *Support Vector Machine*.
3. Serangan yang dideteksi hanya serangan *Man in The Middle* pada dataset.
4. Menggunakan *dataset* yang tercapture *traffic* normal dan serangan *Man in The Middle*.
5. Visualisasi serangan *Man In The Middle* tidak diujikan pada lalu lintas jaringan real-time.
6. pengujian secara *offline*.
7. tidak membahas cara pencegahan serangan *Man in The Middle*.

### **1.6. Metodologi Penelitian**

Metodologi yang digunakan dalam penelitian 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 system deteksi serangan *Man in The Middle* menggunakan algoritma *Support Vector Machine* 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 system 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 Penelitian Tugas Akhir ini adalah sebagai berikut:

**BAB I. PENDAHULUAN**

Bab ini menjelaskan tentang landasan topik penelitian yang meliputi Latar Belakang, Tujuan, Manfaat, Rumusan Masalah, Metodologi Penelitian dan Sistematika Penulisan.

**BAB II. TINJAUAN PUSTAKA**

Bab ini berisi penjelasan dasar teori dari penelitian yaitu *Supervisory Control And Data Acquisition, Intrusion Detection System, Man in The Middle Attack, Support Vector Machine*, dan yang berhubungan dengan penelitian.

**BAB III. METODOLOGI PENELITIAN**

Bab ini menjelaskan bagaimana proses penelitian, tahapan perancangan system dan penerapan metode secara sistematis.

**BAB IV. PENGUJIAN DAN ANALISIS**

Bab ini berisi penjelasan dari hasil pengujian system pada penelitian serta analisis hasil dari data yang didapatkan.

**BAB V. KESIMPULAN DAN SARAN**

Bab ini menjelaskan tentang kesimpulan yang di dapat dari penelitian, serta menjawab tujuan yang hendak dicapai seperti yang tertera pada BAB I, dan memberikan saran untuk penelitian selanjutnya.

## DAFTAR PUSTAKA

- [1] 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.
- [2] 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.
- [3] 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.
- [4] 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.
- [5] P. Radoglou-grammatikis, P. Sarigiannidis, and I. Giannoulakis, “Attacking IEC-60870-5-104 SCADA Systems.”
- [6] 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.
- [7] Y. Yang, K. McLaughlin, T. Littler, S. Sezer, and H. F. Wang, “Rule-based Intrusion Detection System for SCADA networks,” *IET Conf. Publ.*, vol. 2013, no. 623 CP, pp. 2–5, 2013, doi: 10.1049/cp.2013.1729.
- [8] Y. Yang *et al.*, “Multiattribute SCADA-specific intrusion detection system for power networks,” *IEEE Trans. Power Deliv.*, vol. 29, no. 3, pp. 1092–1102, 2014, doi: 10.1109/TPWRD.2014.2300099.
- [9] G. P. Spathoulas and S. K. Katsikas, “Enhancing IDS performance through comprehensive alert post-processing,” *Comput. Secur.*, vol. 37, pp. 176–196, 2013, doi: 10.1016/j.cose.2013.03.005.
- [10] Kamesh and N. Sakthi Priya, “A survey of cyber crimes Yanping,” *Secur. Commun. Networks*, vol. 5, no. June 2011, pp. 422–437, 2012, doi: 10.1002/sec.
- [11] E. Hodo, S. Grebeniuk, H. Ruotsalainen, and P. Tavolato, “Anomali detection for simulated IEC-60870-5-104 traffic,” *ACM Int. Conf. Proceeding Ser.*, vol. Part F1305, 2017, doi: 10.1145/3098954.3103166.

- [12] R. Lily *et al.*, “Diagnosing and Predicting Wind Turbine Faults from SCADA Data Using Support Vector Machines,” pp. 0–11, 2018.
- [13] E. J. M. Colbert, *Security of Industrial Systemm*. .
- [14] S. Boyer, “SCADA - Supervisory Control and Data Acquisition. ISA 3rd Edition.” p. 204, 2004.
- [15] G. Clarke, D. Reynders, and E. Wright, “Practical Modern SCADA Protocols: DNP3, 60870.5 and Related Systems,” *Pract. Mod. SCADA Protoc. DNP3, 60870.5 Relat. Syst.*, vol. (5)2, no. 2, pp. 1–537, 2004, doi: 10.1016/B978-0-7506-5799-0.X5015-3.
- [16] C. Y. Lin and S. Nadjm-Tehrani, “Understanding IEC-60870-5-104 traffic patterns in SCADA networks,” *CPSS 2018 - Proc. 4th ACM Work. Cyber-Physical Syst. Secur. Co-located with ASIA CCS 2018*, pp. 51–60, 2018, doi: 10.1145/3198458.3198460.
- [17] Y. Yang, K. McLaughlin, T. Littler, S. Sezer, B. Pranggono, and H. F. Wang, “Intrusion Detection System for IEC 60870-5-104 based SCADA networks,” *IEEE Power Energy Soc. Gen. Meet.*, no. May 2014, 2013, doi: 10.1109/PESMG.2013.6672100.
- [18] P. Matoušek, O. Ryšavý, and M. Grégr, “Increasing Visibility of IEC 104 Communication in the Smart Grid,” no. December 2015, pp. 21–30, 2019, doi: 10.14236/ewic/icscsr19.3.
- [19] B. Celiktas and M. S. Tok, “TECHNOLOGY MAN IN THE MIDDLE ( MITM ) ATTACK DETECTION TOOL,” no. August, 2018, doi: 10.5281/zenodo.1336698.
- [20] 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*, no. August 2019, pp. 64–69, 2017, doi: 10.1109/ICSSA.2016.19.
- [21] B. Chen, N. Pattanaik, A. Goulart, K. L. Butler-Purry, and D. Kundur, “Implementing attacks for modbus/TCP protocol in a real-time cyber physical system test bed,” *Proc. - CQR 2015 2015 IEEE Int. Work. Tech. Comm. Commun. Qual. Reliab.*, no. June, 2015, doi: 10.1109/CQR.2015.7129084.
- [22] Y. N. Kunang, S. Nurmaini, D. Stiawan, A. Zarkasi, and F. Jasimir, “Automatic Features Extraction Using Autoencoder in Intrusion Detection System,” *Proc. 2018 Int. Conf. Electr. Eng. Comput. Sci. ICECOS 2018*, no. December, pp. 219–224, 2019, doi: 10.1109/ICECOS.2018.8605181.
- [23] N. Sultana, N. Chilamkurti, W. Peng, and R. Alhadad, “Survey on SDN based network intrusion detection system using machine learning approaches,” *Peer-to-Peer Netw.*

- Appl.*, vol. 12, no. 2, pp. 493–501, 2019, doi: 10.1007/s12083-017-0630-0.
- [24] S. Aljawarneh, M. Aldwairi, and M. B. Yassein, “Anomali-based intrusion detection system through feature selection analysis and building hybrid efficient model,” *J. Comput. Sci.*, vol. 25, pp. 152–160, 2018, doi: 10.1016/j.jocs.2017.03.006.
- [25] N. Chaabouni, M. Mosbah, A. Zemmari, C. Sauvignac, and P. Faruki, “Network Intrusion Detection for IoT Security Based on Learning Techniques,” *IEEE Commun. Surv. Tutorials*, vol. 21, no. 3, pp. 2671–2701, 2019, doi: 10.1109/COMST.2019.2896380.
- [26] N. Kaja, A. Shaout, and D. Ma, “An intelligence intrusion detection system,” *Appl. Intell.*, vol. 49, no. 9, pp. 3235–3247, 2019, doi: 10.1007/s10489-019-01436-1.
- [27] S. Akbar, D. K. N. Rao, and D. J. A. Chandulal, “Intrusion Detection System Methodologies Based on Data Analysis,” *Int. J. Comput. Appl.*, vol. 5, no. 2, pp. 10–20, 2010, doi: 10.5120/892-1266.
- [28] S. Kurnaz and I. A. Obaid, “Support Vector Machine ( SVM ) Based on Wavelet Transform ( WT ) for Intrusion Detection System ( IDS ),” vol. 8 pp21, no. 2, pp. 13–19, 2019.
- [29] I. Ahmad, M. Basher, M. J. Iqbal, and A. Rahim, “Performance Comparison of Support Vector Machine, Random Forest, and Extreme Learning Machine for Intrusion Detection,” *IEEE Access*, vol. 6, pp. 33789–33795, 2018, doi: 10.1109/ACCESS.2018.2841987.
- [30] X. Deng, Q. Liu, Y. Deng, and S. Mahadevan, “An improved method to construct basic probability assignment based on the confusion matrix for classification problem,” *Inf. Sci. (Ny).*, vol. 340–341, pp. 250–261, 2016, doi: 10.1016/j.ins.2016.01.033.
- [31] 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.
- [32] 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.