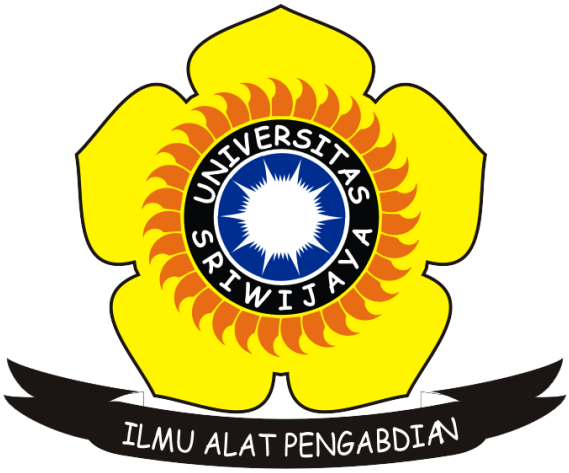
SISTEM DETEKSI SERANGAN *MAN IN THE MIDDLE* (MITM) PADA PROTOKOL JARINGAN IEC 60870-5-104 *SUPERVISORY CONTROL AND DATA ACQUISITION* (SCADA) MENGGUNAKAN METODE NAIVE BAYES

TUGAS AKHIR

Diajukan Untuk Melengkapi Salah Satu Syarat

Memperoleh Gelar Sarjana Komputer



OLEH :

A Josman Pratama

09011381823087

JURUSAN SISTEM KOMPUTER

FAKULTAS ILMU KOMPUTER

UNIVERSITAS SRIWIJAYA

2022

LEMBAR PENGESAHAN

SISTEM DETEKSI SERANGAN *MAN IN THE MIDDLE* (MITM) PADA PROTOKOL JARINGAN IEC 60870-5-104 *SUPERVISORY CONTROL AND DATA ACQUISITION* (SCADA) MENGGUNAKAN METODE NAÏVE BAYES

TUGAS AKHIR

Program Studi Sistem Komputer
Jenjang S1

Oleh

A Josman Pratama

09011381823087

Palembang, Desember 2022

Mengetahui,

Ketua Jurusan Sistem Komputer	Pembimbing Tugas Akhir
Dr. Ir. H. Sukemi, M.T.	**Deris Stiawan, M.T., Ph.D.**
NIP. 196612032006041001	**NIP. 197806172006041002**

HALAMAN PERSETUJUAN

Telah diuji dan lulus pada :

Hari : Jum'at
Tanggal : 11 November 2022

Tim Penguji :

1. **Ketua : Ahmad Zarkasi, S.T., M.T.**
2. **Penguji : Huda Ubaya, S.T., M.T.**
3. **Sekretaris : Tri Wanda Septian, S.Kom., M.Sc.**
4. **Pembimbing : Deris Stiawan, M.T., Ph.D.**

Mengetahui,
Ketua Jurusan Sistem Komputer

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

LEMBAR PERNYATAAN

Yang bertanda tangan dibawah ini:

Nama : A Josman Pratama

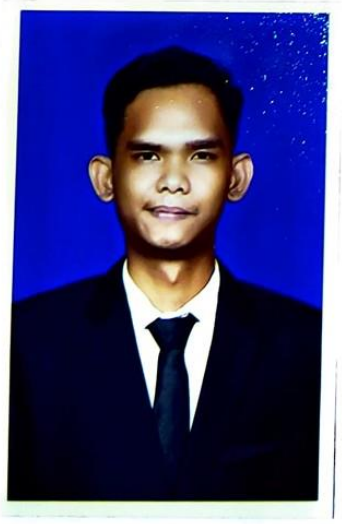
NIM : 09011381823087

Judul : Sistem Deteksi *Serangan Man In The Middle* (MITM) Pada Protokol Jaringan IEC 60870-5-104 *Supervisory Control And Data Acquisition* (SCADA) Menggunakan Metode Naive Bayes

Hasil Pengecekan *Software iThenticate/Turnitin* : 10%

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.



Palembang, Desember 2022

A Josman Pratama

NIM. 09011381823087

HALAMAN PERSEMBAHAN

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيم

Skripsi ini penulis dedikasikan kepada kedua orang tua tercinta, Ayah dan Ibu, ketulusanya dari hati atas doa yang tak pernah putus, semangat yang tak ternilai. Serta untuk orang-orang terdekatku yang tersayang, Dan untuk almamater ku kebanggaanku Program Studi Sistem Komputer Fakultas Ilmu Komputer Universitas Sriwijaya.

Dengan mengucap syukur Alhamdulillah atas rahmat Allah Subhanahu wa Ta'ala yang telah membrikan izin serta ridhonya sehingga penulis mampu memenuhi harapan keluarga besar, rekan seperjuagan, serta civitas akademik agar segera menyelesaikan masa studi untuk mendapatkan gelar sarjana komputer.

"Stop comparing yourself to people who started 10 years before you. Focus on your own journey - Russell Brunson"

"Berhenti membandingkan diri anda dengan orang yang memulai 10 tahun sebelum anda. Fokus pada perjalanan anda sendiri - Russell Brunson"

Desember 2022

KATA PENGANTAR

Assalamualaikum Warahmatullahi Wabarakatuh

Segala puji dan syukur atas kehadirat Tuhan Yang Maha Esa, yang atas segala berkat,kasih sayang,serta karunia-Nya penulis dapat menyelesaikan penulisan proposal tugas akhir ini yang berjudul "**Sistem Deteksi *Serangan Man In The Middle* (MITM) Pada Protokol Jaringan IEC 60870-5-104 *Supervisory Control And Data Acquisition* (SCADA) Menggunakan Metode Naive Bayes "**

Pada penyusunan laporan ini, penulis banyak mendapatkan ide dan saran serta bantuan dari berbagai pihak baik secara langsung maupun tidak langsung. Oleh karena itu, pada kesempatan ini penulis mengucapkan rasa syukur kepada Tuhan Yang Maha Esa dan terimakasih kepada yang terhormat:

1.Kedua orang tua, saudara, dan Keluarga Besar yang selalu mendoakan dan memberikan motivasi dan support

2.Bapak Dr.Ir.Sukemi,M.T. selaku Ketua Jurusan Sistem Komputer Fakultas Ilmu Komputer.

3.Bapak Jaidan Jauhari selaku Dekan Fakultas Ilmu Komputer Universitas Sriwijaya.

4. Bapak Deris Stiawan, M.T., Ph.D. selaku Dosen Pembimbing Tugas Akhir.

5.Mbak Sari selaku Administrasi Jurusan Sistem Komputer yang telah membantu melancarkan proses administrasi terkait Tugas Akhir

6.Seluruh staff dan pegawai jurusan sistem komputer beserta teman seperjuagan yang telah membersamai jalan juang.

7.Dan semua pihak yang telah membantu..

Penulis menyadari bahwa laporan ini masih sangat jauh dari kata sempurna. Untuk itu kritik dan saran yang membangun sangat lah diharapkan penulis agar dapat segera diperbaiki sehingga laporan ini dapat dijadikan sebagai masukkan ide dan pemikiran yang bermanfaat bagi semua pihak dan menjadi tambahan bahan

bacaan bagi yang tertarik dalam penelitian Cyber Attack pada *Supervisory Control And Data Acquisition* (SCADA)

Wassalamualaikum Warahmatullahi Wabarakatuh

Palembang, Desember 2022

Penulis,

A Josman Pratama
NIM. 09011381823087

Man In The Middle (MITM) Attack Detection System on Network Protocol IEC 60870-5-104 Supervisory Control And Data Acquisition (SCADA) Using Naive Bayes Method

A Josman Pratama (09011381823087)
Department of Computer Systems, Faculty of Computer Science, Sriwijaya University
Email : josmanpratama01@gmail.com

ABSTRACT

SCADA is an industrial control system with an access control network that monitors and manages industrial processes remotely. The increasing development of the internet, especially in the industrial world, has also increased the threat of cyber attacks that threaten and endanger the functioning of the SCADA system. The other is the IEC 60870-5-104 (IEC-104) protocol which uses port 2404 (TCP) Transmission Control Protocol, which has a vulnerability that does not include an adequate authorization mechanism, allowing it to be exploited by unauthorized cybercriminals or so-called attacks. MITM. This research will detect MITM attacks, study attack patterns, distinguish normal packets and attack packets, and then calculate the detection system's Accuracy using the Naive Bayes algorithm. The results that get the best performance using the nave Bayes algorithm that applies oversampling smote is to split training data 60%. Data are testing 40%, namely getting a TPR of 94.50, FPR of 15.80, TNR of 84.19, FNR of 05.49, and Accuracy of 88.70.

Keyword : *Supervisory Control and Data Acquisition* (SCADA), *Man In The Middle* (MITM), *Naïve Bayes*

Acknowledge,

Head Of Computer System Departement	**Supervisor**
Dr. Ir. H. Sukemi, M.T.	**Deris Stiawan, M.T., PH.D.**
NIP. 196612032006041001	**NIP. 197806172006041002**

Sistem Deteksi Serangan Man In The Middle (MITM) Pada Protokol Jaringan IEC 60870-5-104 Supervisory Control And Data Acquisition (SCADA) Menggunakan Metode Naive Bayes

A Josman Pratama (09011381823087)
Jurusan Sistem Komputer, Fakultas Ilmu Komputer, Universitas Sriwijaya
Email : josmanpratama01@gmail.com

ABSTRAK

SCADA adalah sistem kendali industri yang memiliki jaringan akses kontrol yang dapat memantau dan mengelolah proses industri dari jarak jauh.Semakin meningkatnya perkembangan internet terutama di dunia industri maka meningkat pula ancaman serangan siber yang mengancam dan membahayakan fungsi dari sistem SCADA.SCADA memiliki standar komunikasi internasional salah satunya adalah protokol IEC 60870-5-104 (IEC-104) yang menggunakan port 2404 (TCP) Transmission Control Protocol,yang memiliki kerentanan dimana tidak menyertakan mekanisme otorisasi yang memadai, sehingga memungkinkan di manfaatkan oleh penjahat siber yang tidak sah atau biasa disebut serangan MITM .Pada penelitian ini akan di lakukan deteksi serangan MITM serta mempelajari pola serangan dan juga membedakan paket normal dan paket serangan kemudian menghitung akurasi dari sistem deteksi tersebut menggunakan algoritma Naive Bayes. Dengan hasil yang mendapatkan performa terbaik menggunakan algoritma naïve bayes yang menerapkan oversampling smote adalah dengan split data training 60% dan data testing 40%, Yaitu memperoleh TPR sebesar 94.50, FPR sebesar 15.80, TNR sebesar 84.19, FNR sebesar 05.49, Accuracy sebesar 88.70.

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

Mengetahui,

Ketua Jurusan Sistem Komputer	**Pembimbing Tugas Akhir**
Dr. Ir. H. Sukemi, M.T.	**Deris Stiawan, M.T., PH.D.**
NIP. 196612032006041001	**NIP. 197806172006041002**

DAFTAR ISI

LEMBAR PENGESAHAN i

KATA PENGANTAR.....v

DAFTAR ISI..... ix

DAFTAR GAMBAR..... xii

DAFTAR TABEL..... xiv

DAFTAR RUMUS xv

BAB 1.....1

PENDAHULUAN.....1

1.1 Latar Belakang..... 1

1.2 Perumusan Masalah..... 2

1.3 Tujuan..... 3

1.4 Manfaat..... 3

1.5 Batasan Masalah..... 3

1.6 Metodelogi Penelitian..... 4

1.7 Sistematika Penulisan..... 5

BAB II 7

TINJAUAN PUSTAKA.....7

2.1 Penelitian Terkait Sebelumnya..... 7

2.2 Diagram Konsep Penelitian..... 8

2.3 SCADA (Supervisory Control And Data Acquisition) 8

2.4 Protocol IEC-60870-5-104 / IEC-104 10

2.5 Application Service Data Unit (ASDU) 11

2.6 Application Protocol Control Information (APCI) 11

2.7 IDS (Intrusion Detection System) 12

2.8 Tipe Klasifikasi IDS 13
2.9 Metode IDS 15
2.10 Man In The Middle (MITM) 15
2.11 Tipe Serangan MITM 16
2.12 SMOTE (Synthetic Minority Oversampling Technique) 18
2.13 Stratified K-Fold 19
2.14 Algoritma Naive Bayes 19
2.15 Evaluasi IDS (Intrusion Detection System) Naïve Bayes 20
BAB III 21
METODOLOGI PENELITIAN 21
3.1 Pendahuluan 21
3.2 Kerangka Kerja Penelitian 21
3.3 Perancangan Sistem 23
3.4 Kebutuhan Perangkat Lunak Penelitian 23
3.5 Dataset *Scada Testbed* 23
3.6 Snort IDS untuk Mendeteksi serangan 24
3.7 Data Exploration and Preparation 26
3.8 Data Extraction 26
3.9 Mengenali pola serangan Man In The Middle 28
3.10 Deteksi serangan menggunakan Naïve Bayes 29
BAB IV 31
HASIL DAN ANALISIS 31
4.1 Pendahuluan 31
4.2 Analisis dataset *Raw packet data (.pcap)* 31
4.3 Serangan *Man In The Middle* yang terdapat pada dataset 32
4.4 *Snort* sebagai *Intrusion Detection System* 32

4.5 Pola serangan *Man In The Middle* 33
4.6 Ekstraksi Dataset 35
4.7 Hasil dari Ekstraksi Dataset 35
4.8 *Oversampling* dataset menggunakan *SMOTE* 38
4.9 Pengujian data dengan *Stratified KFold Cross Validation* 39
4.10 Perhitungan menggunakan *Confusion Matrix* 42
4.11 Hasil sebelum Oversampling SMOTE 48
4.12 Hasil sesudah Oversampling SMOTE 49
BAB V 50
KESIMPULAN DAN SARAN 50
5.1 Kesimpulan 50
5.2 Saran 50
DAFTAR PUSTAKA 52

DAFTAR GAMBAR

Gambar 2.1 Diagram Konsep Penelitian 8
Gambar 2.2 Arsitektur Basic SCADA 9
Gambar 2.3 Format Frame tipe I 10
Gambar 2.4 ASDU 11
Gambar 2.5 APCI 12
Gambar 2.6 Arsitektur IDS 12
Gambar 3.1 Kerangka kerja penelitian 22
Gambar 2.2 Diagram Network Sampel Tesbed 24
Gambar 3.3 Flowchart SNORT IDS 25
Gambar 3.4 Program Data Extraction 27
Gambar 3.5 Hubungan antara snort alert, raw data dan hasil ekstraksi data. 28
Gambar 3.6 Flowchart program Naïve Bayes 30
Gambar 4.1 Raw Packet data (.pcap) 31
Gambar 4.2 Rules snort 32
Gambar 4.3 Alert Snort 33
Gambar 4.4 Paket trafik normal IEC 104 33
Gambar 4.5 Paket trafik serangan IEC 104 34
Gambar 4.6 IEC 104 Valid Cots 34
Gambar 4.7 Dataset CSV 35
Gambar 4.8 Korelasi antara raw data dan hasil ekstraksi normal 35
Gambar 4.9 Korelasi antara raw data dan hasil ekstraksi serangan 36
Gambar 4.10 Data sebelum Oversampling SMOTE 38
Gambar 4.11 Data sesudah Oversampling SMOTE 38
Gambar 4.12 Hasil Rata-Rata Akurasi *Stratified KFold Cross Validation* 41
Gambar 4.13 Hasil Confusion Matrix sebelum Oversampling di SMOTE 80% dan 20% 41
Gambar 4.14 Hasil Confusion Matrix Oversampling sebelum di SMOTE 70% ... dan 30% 42
Gambar 4.15 Hasil Confusion Matrix Oversampling sebelum di SMOTE 60% ... dan 40% 42

Gambar 4.16 Hasil Confusion Matrix Oversampling sesudah di SMOTE 80%.... dan 20%..... 43
Gambar 4.17 Hasil Confusion Matrix Oversampling sesudah di SMOTE 70%.... dan 30%..... 44
Gambar 4.18 Hasil Confusion Matrix Oversampling sesudah di SMOTE 60% dan 40%..... 44

DAFTAR TABEL

Table 2.1 Confusion Matrix 20
Table 2.2 Alert Confusion Matrix 20
Table 3.1 Kerangka kerja penelitian..... 23
Table 3.2 Kebutuhan Perangkat Lunak Penelitian 23
Table 3.3 Atribut IEC 104..... 26
Table 4.1 fitur yang di ekstraksi..... 37
Table 4.2 Hasil Pengujian data dengan Stratified Kfold Cross Validation..... 39
Table 4.3 Hasil Confusion Matrix sebelum Oversampling SMOTE 48
Table 4.4 Hasil Detection Rate Confusion Matrix sebelum Oversampling SMOTE 48
Table 4.5 Hasil Confusion Matrix sesudah Oversampling SMOTE 49
Table 4.6 Hasil Detection Rate Confusion Matrix sesudah Oversampling SMOTE 49
Table 4.7 Hasil Terbaik Confusion Matrix sesudah Oversampling SMOTE..... 49

DAFTAR RUMUS

Rumus 1 Stratified KFold 18
Rumus 2 Naïve Bayes 18
Rumus 3 Accuracy 20
Rumus 4 True Positif Rate 20
Rumus 5 False Positif Rate 20
Rumus 6 True Negatife Rate.....20
Rumus 7 False Negatif Rate 20
Rumus 8 Precision.....20

BAB 1

PENDAHULUAN

1.1 Latar Belakang

Supervisory Control and Data Acquisition atau biasa di singkat (*SCADA*) menurut Y. Cherdantseva [1] adalah sistem kendali industri yang memiliki jaringan akses kontrol yang dapat memantau dan mengelolah proses industri dari jarak jauh.Semakin meningkatnya perkembangan internet terutama di dunia industri maka meningkat pula ancaman serangan siber yang mengancam dan membahayakan fungsi dari sistem *SCADA*. Sistem *SCADA* memiliki komponen perangkat keras dan perangkat lunak dan juga memiliki jaringan penghubung.Arsitekturnya dibentuk oleh perangkat *Remote Terminal Unit (RTU),Intelligent Electronic Device(IED)* dan *Programmable Logic Controller (PLC)* yang saling terhubung oleh infrastruktur komunikasi. *SCADA* [2] banyak digunakan di industri untuk kontrol pengawasan dan akuisisi data proses industri. Prosesnya bisa industri, infrastruktur atau fasilitas.

Berdasarkan penelitian sebelumnya oleh [3] Kemajuan teknologi dalam perangkat komunikasi dan berbagi data berkecepatan tinggi telah membuat sistem *SCADA* semakin rentan terhadap banyak permukaan serangan yang dapat dieksploitasi oleh aktor ancaman, memungkinkan mereka untuk merancang serangan canggih yang parah. Beberapa literatur dan dokumen pemerintah telah menyoroti fakta bahwa infrastruktur penting seperti jaringan listrik semakin menjadi target konstan serangan terkait dunia maya.

Penelitian lainya [4] juga mengatakan bahwa seiring meningkatnya jumlah perangkat lapangan dan node komputasi yang saling terhubung, serangan cyber berbasis jaringan telah menjadi ancaman cyber utama bagi infrastruktur pada jaringan ICS. Perangkat lapangan dan node komputasi di Indrustial Control Systems menjadi sasaran serangan jaringan konvensional dan serangan khusus yang sengaja dibuat untuk protokol jaringan *SCADA*

SCADA memiliki standar komunikasi internasional menurut [5] salah satunya yang digunakan pada penelitian ini adalah protokol IEC 60870-5-104 (IEC-104) yang menggunakan port 2404 *(TCP) Transmission Control Protocol* , yang

memiliki kerentanan dimana tidak menyertakan mekanisme otorisasi yang memadai, sehingga memungkinkan di manfaatkan oleh penjahat siber yang tidak sah atau biasa disebut serangan *MITM (Man In The Middle)*

Pada penelitian tugas akhir skripsi ini berfokus pada serangan siber yang terjadi pada *SCADA* serangan itu adalah *MITM (Man In The Middle)* yang menurut [6] ialah jenis serangan yang terjadi dimana *attacker* / pihak ketiga yang memiliki niat jahat secara diam-diam mengambil kendali saluran komunikasi, *Attacker* biasanya intercept/mencegat, modify/memodifikasi, dan bahkan mengubah *communication traffic* korban.Selain itu, korban juga tidak akan menyadari ada nya penyusup, sehingga korban merasa bahwa komunikasi mereka sudah aman.

Percobaan ini akan menggunakan algoritma *Naive Bayes* untuk mendekteksi serangan *MITM (Man In The Middle)* . *Naive Bayes* merupakan algoritma yang menggunakan pendekatan statistik dalam mengambil keputusan. Algoritma *Naive Bayes* didasarkan pada *Teorema Bayes* bahwa semua atribut berkontribusi sama pentingnya dan terlepas dari kelas tertentu. Keuntungan menggunakan *Naive Bayes* adalah menurut [7] metode ini hanya membutuhkan sedikit data latih untuk menentukan estimasi parameter yang dibutuhkan dalam proses klasifikasi. Naive Bayes sering tampil jauh lebih baik dalam situasi dunia nyata yang paling kompleks daripada yang diharapkan.Berdasarkan hasil pembahasan diatas maka penelitian yang dibuat penulis akan berfokus mempelajari pola serangan *MITM (Man In The Middle*) untuk mendeteksi serangan tersebut menggunakan algoritma *Naive Bayes.*

1.2 Perumusan Masalah

1. Bagaimana cara mengesktrak dataset serangan *MITM* pada protokol jaringan *SCADA* dari *pcap* menjadi *csv*
2. Bagaimana mengenali pola serangan *MITM* pada protokol jaringan *SCADA?*
3. Bagaimana membedakan paket normal dan paket serangan *MITM* pada protokol jaringan *SCADA*?

1.3 Tujuan

Tujuan dari penulisan tugas akhir ini, yaitu :

1. Mendeteksi dan menganalisis serangan *MITM* di protokol jaringan *SCADA* menggunakan *snort* dan mengklasifikasikan nya menggunakan algoritma *Naïve Bayes*

2. Mempelajari Pola traffik dari *MITM* di protokol jaringan *SCADA* menggunakan *snort*

3. Membedakan paket normal dan paket serangan untuk dapat mendeteksi *MITM* di protokol jaringan *SCADA* menggunakan *snort*

4. Menghitung/mengukur kinerja akurasi dari *IDS (Intrusion Detection System)* untuk mendeteksi serangan *MITM* di protokol jaringan *SCADA* menggunakan algoritma *Naïve Bayes*

1.4 Manfaat

Manfaat dari penulisan tugas akhir ini, yaitu :

1. Dapat mendeteksi dan menganalisis serangan *MITM* di protokol jaringan *SCADA* menggunakan *snort* dan mengklasifikasikan nya menggunakan algoritma *Naïve Bayes*

2. Dapat mempelajari Pola traffik dari *MITM* di protokol jaringan *SCADA* menggunakan *snort*

3. Dapat membedakan paket normal dan paket serangan untuk dapat mendeteksi *MITM* di protokol jaringan *SCADA* menggunakan *snort*

4. Dapat menghitung/mengukur kinerja akurasi dari *IDS (Intrusion Detection System)* untuk mendeteksi serangan *MITM* di protokol jaringan *SCADA* menggunakan algoritma *Naïve Bayes*

1.5 Batasan Masalah

Berikut batasan masalah dari tugas akhir ini, yaitu :

1. Dataset yang digunakan pada peneltian ini berasal dari *Figshare*

2. Algoritma yang digunakan untuk melakukan klasifikasi yaitu algoritma *Naïve Bayes*

3. Jenis serangan yang akan dideteksi yaitu serangan *MITM* (*Man In The Middle)*

4. Tidak membahas/mengulas bagaimana cara untuk melakukan prevention/pencegahan terhadap serangan *MITM (Man In The Middle)*

5. Hanya mendeteksi di protokol IEC-104

6. Pengujian dilakukan secara offline

1.6 Metodelogi Penelitian

Pada tugas akhir ini menggunakan metodelogi sebagai berikut :

1. Metode Studi Pustaka dan Literature

Di tahap ini melakuakn studi pustaka serta literature untuk mencari informasi terkati serangan *MITM (Man In The Middle), IDS (Intrusion Detection System), protokol IEC 60870-5-104, SUPERVISORY CONTROL AND DATA ACQUISITION (SCADA)* dan *machine learning***,** dengan cara membaca referensi dari jurnal ilmiah yang nantinya akan digunakan juga untuk penulisan pada laporan tugas akhir skripsi.

2. Metode Perancangan Sistem

Pada tahap ini merancang serta membuat *IDS (Intrusion Detection System)* untuk mendeteksi *MITM (Man In The Middle)* di jaringan *SCADA* menggunakan *Naïve Bayes Algorithm* dan menentukan perangkat yang akan digunakan nanti pada saat penelitian, baik itu dari sisi software maupun dari sisi hardware.

3. Metode Pengujian

Pada tahap ini akan melakukan analisis terhadap perancangan sistem yang sudah di lakukan sebelumnya, untuk dapat mengetahui kinerja dari sistem yang sudah di rancang sebelumnya.

4. Metode Analisis dan Kesimpulan

Pada tahap ini membuat kesimpulan berdasarkan apa yang sudah dikerjakan dan di analisis sebelumnya. Dan juga hasil peneltian ini dapat memberi saran apa saja yang bisa di lakukan oleh penelitian selanjutnya yang tertarik meneliti pada topik ini.

1.7 Sistematika Penulisan

Sistematika penulisan yang digunakan pada tugas akhir skripsi ini adalah sebagai berikut:

BAB I. PENDAHULUAN

Pada Bab I membahas latar belakang, perumusan masalah, tujuan serta manfaat,metodologi penelitian dan sistematika penulisan.

BAB II. TINJAUAN PUSTAKA

Pada Bab II membahas dasar teori dari *(Man In The Middle), IDS (Intrusion Detection System), protokol IEC 60870-5-104, SUPERVISORY CONTROL AND DATA ACQUISITION (SCADA)*, dan *machine learning*

BAB III. METODOLOGI PENELITIAN

Pada Bab III membahas sistem deteksi serta analisis dari serangan MITM (Man In The Middle) di jaringan SCADA menggunakan Naïve Bayes Algorithm

BAB IV. IMPLEMENTASI PENGUJIAN

Pada Bab IV membahas bagaimana proses meng-implementasi sistem deteksi yang sudah dibuat untuk deteksi dari serangan MITM (Man In The Middle) di jaringan SCADA menggunakan Naïve Bayes Algorithm

BAB V. KESIMPULAN DAN SARAN

Pada Bab V mebahas kesimpulan berdasarkan apa yang sudah dikerjakan dan di analisis sebelumnya dan juga membahas hasil dari meng-

implementasikan Naïve Bayes Algorithm dalam mendeteksi MITM (Man In The Middle) serta memberi saran apa saja yang bisa di lakukan oleh penelitian selanjutnya yang tertarik meneliti pada topik ini.

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. N. Lakhoua, "Cyber Security of SCADA Network in Thermal Power Plants," *2018 Int. Conf. Smart Appl. Commun. Networking, SmartNets 2018*, pp. 1–4, 2018, doi: 10.1109/SMARTNETS.2018.8707398.

[3] V. K. Singh, H. Ebrahem, and M. Govindarasu, "Security Evaluation of Two Intrusion Detection Systems in Smart Grid SCADA Environment," *2018 North Am. Power Symp. NAPS 2018*, pp. 1–6, 2019, doi: 10.1109/NAPS.2018.8600548.

[4] H. Yang, L. Cheng, and M. C. Chuah, "Deep-Learning-Based Network Intrusion Detection for SCADA Systems," *2019 IEEE Conf. Commun. Netw. Secur. CNS 2019*, pp. 1–7, 2019, doi: 10.1109/CNS.2019.8802785.

[5] P. R. Grammatikis, P. Sarigiannidis, A. Sarigiannidis, D. Margounakis, A. Tsiakalos, and G. Efstathopoulos, "An Anomaly Detection Mechanism for IEC 60870-5-104," *2020 9th Int. Conf. Mod. Circuits Syst. Technol. MOCAST 2020*, pp. 0–3, 2020, doi: 10.1109/MOCAST49295.2020.9200285.

[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] F. F. Setiadi, M. W. A. Kesiman, and K. Y. E. Aryanto, "Detection of dos attacks using naive bayes method based on internet of things (iot)," *J. Phys. Conf. Ser.*, vol. 1810, no. 1, 2021, doi: 10.1088/1742-6596/1810/1/012013.

[8] S. Tamy, H. Belhadaoui, M. A. Rabbah, N. Rabbah, and M. Rifi, "AN EVALUATION OF MACHINE LEARNING ALGORITHMS," *2019 7th Mediterr. Congr. Telecommun.*, pp. 1–5, 2019.

[9] R. L. Perez, F. Adamsky, R. Soua, and T. Engel, “Machine Learning for Reliable Network Attack Detection in SCADA Systems,” *2018 17th IEEE Int. Conf. Trust. Secur. Priv. Comput. Commun. 12th IEEE Int. Conf. Big Data Sci. Eng.*, pp. 633–638, 2018, doi: 10.1109/TrustCom/BigDataSE.2018.00094.

[10] B. S. Sharmila and R. Nagapadma, “Intrusion detection system using naive bayes algorithm,” *2019 5th IEEE Int. WIE Conf. Electr. Comput. Eng. WIECON-ECE 2019 - Proc.*, pp. 8–11, 2019, doi: 10.1109/WIECON-ECE48653.2019.9019921.

[11] D. D. B, S. R. Chakraborty, and M. Lagineni, *Security Analysis of MITM Attack on SCADA Network*, vol. 1. Springer Singapore, 2020. doi: 10.1007/978-981-15-6318-8.

[12] G. Yadav and K. Paul, “International Journal of Critical Infrastructure Protection Architecture and security of SCADA systems : A review,” *Int. J. Crit. Infrastruct. Prot.*, vol. 34, p. 100433, 2021, doi: 10.1016/j.ijcip.2021.100433.

[13] 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.

[14] 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.

[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] M. Conti, N. Dragoni, and V. Lesyk, “A Survey of Man In The Middle Attacks,” no. c, pp. 1–26, 2016, doi: 10.1109/COMST.2016.2548426.

[17] 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.

[18] 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.

[19] N. A. Diamantidis, D. Karlis, and E. A. Giakoumakis, “Unsupervised stratification of cross-validation for accuracy estimation,” *Artif. Intell.*, vol. 116, no. 1–2, pp. 1–16, 2000, doi: 10.1016/S0004-3702(99)00094-6.

[20] A. C. M. & S. Guido, “Introduction to Machine Learning with Python: A Guide for Data Scientists,” 2013.

[21] P. Maynard, K. McLaughlin, and S. Sezer, “An Open Framework for Deploying Experimental SCADA Testbed Networks,” pp. 92–101, 2018, doi: 10.14236/ewic/ics2018.11.

[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] M. A. S. Arifin, “Malicious Activity Recognition on SCADA Network IEC 60870-5-104 Protocol,” vol. 104, no. Iec 104, pp. 46–51, 2021.

[24] P. Matoušek, “Description and analysis of IEC 104 Protocol Technical Report,” 2017.