DETEKSI SERANGAN *MAN IN THE MIDDLE* (MITM) PADA PROTOKOL JARINGAN IEC 61850 *SUPERVISORY CONTROL AND DATA ACQUISITION* (SCADA) DENGAN MENGGUNAKAN METODE *LONG SHORT TERM MEMORY* (LSTM)

SKRIPSI

Diajukan Untuk Melengkapi Salah Satu Syarat

Memperoleh Gelar Sarjana

Oleh:

Fajar Pradika

09011282126045

JURUSAN SISTEM KOMPUTER

FAKULTAS ILMU KOMPUTER

UNIVERSITAS SRIWIJAYA

2025

HALAMAN PENGESAHAN

SKRIPSI

DETEKSI SERANGAN *MAN IN THE MIDDLE* (MITM) PADA PROTOKOL JARINGAN IEC 61850 *SUPERVISORY CONTROL AND DATA ACQUISITION* (SCADA) DENGAN MENGGUNAKAN METODE *LONG SHORT TERM MEMORY* (LSTM)

Sebagai salah satu syarat untuk penyelesaian studi
di Program Studi S1 Sistem Komputer

OLEH:

FAJAR PRADIKA

09011282126045

Pembimbing 1 : **Prof. Ir. Deris Stiawan, M.T., Ph.D.**
NIP. 197806172006041002

Pembimbing 2 : **Nurul Afifah, M.Kom**
NIP. 199211102023212049

Mengetahui,

Ketua Program Studi Sistem Komputer

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

NIP. 196612032006041001

AUTHENTICATION PAGE

SKRIPSI

MAN IN THE MIDDLE (MITM) ATTACK DETECTION ON IEC 61850 SUPERVISORY CONTROL AND DATA ACQUISITION (SCADA) NETWORK PROTOCOL USING LONG SHORT TERM MEMORY (LSTM)

As one of the requirements for completing studies
in the S1 Computer System Study Program

BY:

FAJAR PRADIKA

09011282126045

Advisor 1 : **Prof. Ir. Deris Stiawan, M.T., Ph.D.**
NIP. 197806172006041002

Advisor 2 : **Nurul Afifah, M.Kom**
NIP. 199211102023212049

Approved by,

Head of the Computer Systems Departement

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

NIP. 196612032006041001

LEMBAR PERSETUJUAN

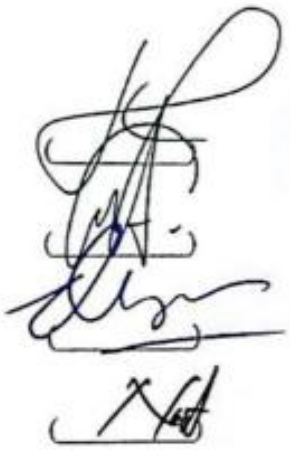
Telah diuji dan lulus pada :

Hari : Jumat

Tanggal : 13 Juni 2025

Tim Penguji

1. Ketua : Huda Ubaya, M.T.
2. Penguji : Dr. Ahmad Zarkasi, M.T.
3. Pembimbing 1 : Prof. Ir. Deris Stiawan, M.T., Ph.D.
4. Pembimbing 2 : Nurul Afifah, M.Kom



Mengetahui

Ketua Jurusan Sistem Komputer

Dr. Ir. Sukemi, M.T.

NIP. 196612032006041001

iv

HALAMAN PERNYATAAN

Yang bertanda tangan dibawah ini :

Nama : Fajar Pradika

NIM : 09011282126045

Judul : Deteksi serangan *Man In The Middle* (MITM) pada protokol jaringan IEC 61850 *Supervisory Control and Data Acquisition* (SCADA) dengan menggunakan metode *Long Short Term Memory* (LSTM)

Hasil Pengecekan Plagiat/Turnitin : 5%

Menyatakan bahwa laporan tugas akhir saya merupakan hasil karya saya sendiri dan bukan hasil penjiplakan/plagiat.Apabila ditemukan unsur penjiplakan/plagiat dalam laporan tugas akhir ini, maka saya bersedia menerima sanksi akademik dari Universitas Sriwijaya.

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

Palembang, 30 Juni 2025

Fajar Pradika

NIM. 09011282126045

v

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) Pada Protokol Jaringan IEC 16850 *Supervisory Control And Data Acquisition* (SCADA) Dengan Menggunakan *Long Short Term Memory* (LSTM)"**.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 Prof. Dr. Erwin, S.Si, M.Si. 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 Prof. Ir. Deris Stiawan, M.T., Ph.D. selaku Dosen Pembimbing Tugas Akhir di Jurusan Sistem Komputer Fakultas Ilmu Komputer Universitas Sriwijaya.
5. Ibu Nurul Afifah, M.Kom selaku Dosen Pembimbing II Tugas Akhir di Jurusan Sistem Komputer Fakultas Ilmu Komputer Universitas Sriwijaya.

6. Bapak Dr. Firdaus, M.Kom. selaku Dosen Pembimbing Akademik di Jurusan Sistem Komputer Fakultas Ilmu Komputer Universitas Sriwijaya.
7. Kak Angga selaku admin Jurusan Sistem Komputer yang telah membantu mengurus seluruh berkas.
8. Seluruh dosen, staff, serta karyawan Fakultas Ilmu Komputer Universitas Sriwijaya.
9. Seluruh pihak yang tergabung dalam COMNETS terutama Syahrul dan bapak Tasmi, S.Kom., M.Kom yang membantu penulis dalam penelitian ini.
10. Teman–teman seperjuangan Jurusan Sistem Komputer Angkatan 2021.
11. Teman–teman saya yang tergabung dalam Grup Kape Ter OP yang selalu memberikan dukungan kepada penulis.
12. Seluruh teman-teman seperjuangan semuanya yang saling membantu dalam hal apapun.
13. Jurusan Sistem Komputer
14. Almamater

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, 30 Juni 2025

Fajar Pradika

NIM. 09011282126045

DETEKSI SERANGAN *MAN IN THE MIDDLE* (MITM) PADA PROTOKOL JARINGAN IEC 61850 *SUPERVISORY CONTROL AND DATA ACQUISITION* (SCADA) DENGAN MENGGUNAKAN METODE *LONG SHORT TERM MEMORY* (LSTM)

FAJAR PRADIKA (09011282126045)

Jurusan Sistem Komputer, Fakultas Ilmu Komputer,

Universitas Sriwijaya

Email : 09011282126045@student.unsri.ac.id

ABSTRAK

Serangan *Man In The Middle* (MITM) adalah ancaman keamanan pada komunikasi jaringan yang memungkinkan penyerang mencegat dan mengubah data yang dikirim antara dua perangkat. Serangan ini dapat mengganggu sistem tenaga listrik berbasis SCADA, dan ini terjadi pada protokol komunikasi IEC 61850, khususnya *Generic Object-Oriented Substation Event* (GOOSE). Penelitian ini menggunakan Dataset diperoleh dari hasil simulasi serangan MITM dan terdiri dari dua kelas, yaitu normal dan serangan dengan menggunakan metode *Long Short-Term Memory* (LSTM) untuk mendeteksi serangan MITM pada protokol GOOSE. Hasil penelitian menunjukkan bahwa metode LSTM efektif dalam mendeteksi serangan MITM dengan performa yang baik.Model terbaik dan stabil diperoleh pada konfigurasi dengan pembagian data 80:20 dan 200 *epoch*,menghasilkan akurasi sebesar 95.96%, *precision* 93.33%, *recall* 99,96%, dan *f1-score* 96.17%.

Kata Kunci : *Supervisory Control and Data Acquisition, Man In The Middle, IEC 61850, Long Short Term Memory*

MAN IN THE MIDDLE (MITM) ATTACK DETECTION ON IEC 61850 SUPERVISORY CONTROL AND DATA ACQUISITION (SCADA) NETWORK PROTOCOL USING LONG SHORT TERM MEMORY (LSTM)

FAJAR PRADIKA (09011282126045)

Dept. Of Computer System, Faculty of Computer Science,

Sriwijaya University

Email : 09011282126045@student.unsri.ac.id

ABSTRACT

A Man-in-the-Middle (MITM) attack is a security threat in network communication that allows an attacker to intercept and modify data transmitted between two devices. This attack can disrupt SCADA-based power systems and occurs in the IEC 61850 communication protocol, particularly in the Generic Object-Oriented Substation Event (GOOSE) protocol.This study utilizes a dataset obtained from MITM attack simulations, consisting of two classes: normal and attack. The Long Short-Term Memory (LSTM) method is applied to detect MITM attacks in the GOOSE protocol.The results show that the LSTM method is effective in detecting MITM attacks with good performance.The best and most stable model configuration was achieved with an 80:20 data split and 200 epochs, yielding an accuracy of 95.96%, precision of 93.33%, recall of 99.19%, and an F1-score of 96.17%.

Keyword : *Supervisory Control and Data Acquisition, Man In The Middle, IEC 61850, Long Short Term Memory*

DAFTAR ISI

HALAMAN PENGESAHAN ..... **ii**
AUTHENTICATION PAGE ..... **iii**
LEMBAR PERSETUJUAN ..... **iv**
HALAMAN PERNYATAAN ..... **v**
KATA PENGANTAR ..... **vi**
ABSTRAK ..... **viii**
ABSTRACT ..... **ix**
DAFTAR ISI ..... **x**
DAFTAR GAMBAR ..... **xii**
DAFTAR TABEL ..... **xiv**
BAB I PENDAHULUAN **1**
1.1 Latar belakang 1
1.2 Rumusan Masalah 3
1.3 Tujuan 4
1.4 Manfaat 4
1.5 Batasan Masalah 4
1.6 Sistematika penelitian 5
BAB II TINJAUAN PUSTAKA **6**
2.1 Penelitian Terkait 6
2.2 *Supervisory Control And Data Acquisition* (SCADA) 12
2.3 Protokol GOOSE IEC 61850 13
2.4 *Man In The Middle* (MITM) 14
2.5 *Deep Learning* 15
2.6 *Long Short Term Memory (LSTM)* 15
2.7 *Data Balencing* 16
2.8 *Confusion Matrix* 17
BAB III METODOLOGI PENELITIAN **18**
3.1 Pendahuluan 18
3.2 Kerangka Kerja Penelitian 18
3.3 Perancangan Sistem 20
3.3.1 Pembuatan Data Set 20
3.3.2 Pemilihan Peralatan Hardware dan software 21
3.3.3 Topologi Serangan 22
3.3.4 Konfigurasi GOOSE 22

3.3.5 Skenario serangan 24
3.4 Data ekstraksi 25
3.5 Preprosesing 26
3.5.1 Label Data 26
3.5.2 Seleksi Fitur 27
3.5.3 Data Balencing 27
3.5.4 *Split Dataset* 28
3.6 Penerapan Algoritma *Long Short Term Memory* (LSTM) 29
3.6.1 Arsitektur Model LSTM 30
3.7 Validasi Model 31
BAB IV HASIL DAN PEMBAHASAN 33
4.1 Pendahuluan 33
4.2 Pembuatan Dataset 33
4.2.1 Konfigurasi GOOSE 33
4.2.2 Pengujian Data Normal 34
4.2.3 Pengujian Data Serangan 36
4.3 Data ekstraksi 40
4.4 *Preprosesing* 41
4.4.1 Label data 41
4.4.2 Seleksi Fitur 42
4.4.3 Data Balancing 42
4.4.4 *Split Dataset* 44
4.5 Penerapan Model LSTM 44
4.6 Evaluasi Model 45
4.6.1 Hasil Skala Percobaan 1 45
4.6.2 Hasil Skala Percobaan 2 48
4.6.3 Hasil Skala Percobaan 3 50
4.6.4 Hasil Skala Percobaan 4 52
4.6.3 Hasil Skala Percobaan 5 54
4.7 Validasi Perhitungan Manual LSTM 57
4.8 Analisis Hasil Percobaan 61
BAB V KESIMPULAN DAN SARAN 63
Kesimpulan 63
Saran 64
DAFTAR PUSTAKA 65

DAFTAR GAMBAR

Gambar 2.1 Keyword Analysis.....11
Gambar 2.2 Arsitektur Scada..... 12
Gambar 2.3 Struktur sistem kontrol ICS 13
Gambar 2.4 Struktur Jaringan IEC 61850 13
Gambar 2.5 MITM Attack. 14
Gambar 2.6 Deep Learning 15
Gambar 2.7 Arsitektur LSTM..... 19
Gambar 3.1 Kerangka Kerja..... 19
Gambar 3.2 Pembuatan dataset 21
Gambar 3.3 Topologi Serangan MITM 22
Gambar 3.4 Konfigurasi GOOSE..... 23
Gambar 3.5 Skenario serangan..... 24
Gambar 3.6 Data ekstraksi..... 25
Gambar 3.7 *Preprosesing* 26
Gambar 3.8 *Flowchart* data *balancing*..... 28
Gambar 3.9 Penerapan algoritma LSTM..... 29
Gambar 3.10 Arsitektur Pemodelan LSTM..... 30
Gambar 4.1 Konfigurasi Goose berhasil 33
Gambar 4.2 Frekuensi Aplikasi percobaan 1..... 34
Gambar 4.3 Frekuensi Aplikasi percobaan 2..... 35
Gambar 4.4 Frekuensi Aplikasi percobaan 3..... 35
Gambar 4.5 Frekuensi Aplikasi percobaan 4..... 35
Gambar 4.6 Frekuensi Aplikasi percobaan 5..... 36
Gambar 4.7 MITM Mengubah APPID..... 38
Gambar 4.8 Frekuensi Aplikasi percobaan 1..... 39
Gambar 4.9 Frekuensi Aplikasi percobaan 2..... 39
Gambar 4.10 Frekuensi Aplikasi percobaan 3..... 39
Gambar 4.11 Frekuensi Aplikasi percobaan 4..... 40
Gambar 4.12 Frekuensi Aplikasi percobaan 5..... 40
Gambar 4.13 Data ekstraksi..... 41
Gambar 4.14 Data Setelah diberi label..... 41

Gambar 4.15 Data Setelah Seleksi Fitur 42
Gambar 4.16 Sebelum Data Balancing 42
Gambar 4.17 Setelah *Data Balancing* 43
Gambar 4.18 *Split Dataset* 44
Gambar 4.19 *Training Model* 45
Gambar 4.20 *Training & Validation Loss* Skala percobaan 1 46
Gambar 4.21 *Confusion Matrix* Skala percobaan 1 47
Gambar 4.22 *Training & Validation Loss* Skala percobaan 2 48
Gambar 4.23 *Confusion Matrix* Skala percobaan 2 49
Gambar 4.24 *Training & Validation Loss* Skala percobaan 3 50
Gambar 4.25 *Confusion Matrix* Skala percobaan 3 51
Gambar 4.26 *Training & Validation Loss* Skala percobaan 4 53
Gambar 4.27 *Confusion Matrix* Skala percobaan 4 53
Gambar 4.28 *Training & Validation Loss* Skala percobaan 5 55
Gambar 4.29 *Confusion Matrix* Skala percobaan 5 56
Gambar 4.30 Arsitektur Model *Sequential* LSTM 57

DAFTAR TABEL

Tabel 2.1 Matrix Penelitian Terkait 6
Tabel 3.1 Spesifikasi Hardware 21
Tabel 3.2 Spesifikasi software 22
Tabel 3.3 Validasi *Hyperparameter Tunning* 32
Tabel 4.1 Percobaan Paket Normal 34
Tabel 4.2 Percobaan Paket MITM 36
Tabel 4.3 Sebelum *Data Balancing* 42
Tabel 4.4 Setelah *Data Balancing* 43
Tabel 4.5 Perbandingan Data Training dan Testing 44
Tabel 4.6 Metrik Evaluasi Model Skala 1 46
Tabel 4.7 Metrik Evaluasi Model Skala 2 48
Tabel 4.8 Metrik Evaluasi Model Skala 3 50
Tabel 4.9 Metrik Evaluasi Model Skala 4 52
Tabel 4.10 Metrik Evaluasi Model Skala 5 55

BAB I
PENDAHULUAN

1.1 Latar belakang

Supervisory Control and Data Acquisition (SCADA) adalah sistem yang digunakan untuk pemantauan dan pengontrolan industri dari pusat guna untuk menganalisis dan mengumpulkan data [1].Menurut penelitian yang dilakukan oleh [2] Saat ini, SCADA telah diintegrasikan ke dalam infrastruktur kritis seperti pembangkit listrik, sistem transportasi, distribusi air, dan pengelolaan air limbah untuk memantau dan mengontrol proses-proses tersebut.

Menurut[3],Protokol IEC 61850 merupakan salah satu protokol yang digunakan dalam *Supervisory Control and Data Acquisition* (SCADA) yang dirancang untuk meningkatkan efisiensi komunikasi dalam pengoprasian sistem jaringan listrik dengan pertukaran data yang cepat dan akurat.Dalam penelitian [1] juga menjelaskan bahwa salah satu komponen penting dalam otomasi gardu induk pada standar ini adalah komunikasi *Generic Object-Oriented Substation Event* (GOOSE) yang merupakan protokol komunikasi berbasis pesan dan memastikan pertukaran data cepat antar perangkat *Intellgent Electronic Devices* (IEDs) dalan sistem operasional gardu induk yang membuat sistem tenaga listrik beroprasi lebih efisien, aman, dan stabil.

Meskipun dirancang untuk kecepatan dan efisiensi,Penelitian [4] menjelaskan tentang protokol *Generic Object-Oriented Substation Events* (GOOSE) IEC 61850 memiliki kerentanan yang signifikan terhadap serangan siber dari dalam maupun luar jaringan.Penggunaan enkripsi yang tinggi dapat menyebabkan latensi yang tidak dapat diterima dalam komunikasi GOOSE.Terdapat banyak macam jenis serangan yang dapat dapat diterima dalam komunikasi GOOSE diantaranya yang paling paling umum adalah serangan Dos dan MITM,pada penilitian [5] membahas tentang serangan Dos yang menginjeksi Protokol komunikasi pada gardu berbasis IEC 61850, selanjutnya adalah serangan yang akan menjadi fokus utama dari penelitian ini, yaitu *Man In The Middle Attack* (MITM).

Dijelaskan pada penelitian [6] serangan *Man In The Middle Attack* (MITM) attack adalah jenis serangan di mana penyerang dapat mencegat dan memanipulasi

komunikasi antara dua pihak tanpa diketahui yang dimana penyerang dapat melakukan pengintaian atau mengubah data yang dikirimkan.Penelitian ini juga menyebutkan [6] penyerang tidak hanya mengawasi tetapi juga memodifikasi data yang dikirimkan, yang dapat menyebabkan menyebabkan kebocoran informasi sensitif, pencurian data, dan kerusakan integritas data.Dampak tersebut sangat berbahaya, penelitian [7] menyebutkan bahwa protokol-protokol dalam IEC 61850, seperti MMS, GOOSE, dan SV, tidak memiliki fitur keamanan penting terkait kerahasiaan, integritas, dan otentikasi, yang membuatnya rentan terhadap serangan MITM.

Beberapa penelitian sebelumnya telah mengusulkan pendekatan berbasis pembelajaran mesin untuk mendeteksi anomali pada protokol IEC 61850,pada penelitian [8] Sistem deteksi intrusi berbasis *machine learning* dirancang untuk meningkatkan keamanan siber smart grid menggunakan pesan GOOSE IEC 61850 dengan memantau lalu lintas komunikasi dan mendeteksi serangan siber menggunakan metode seperti *Random Forest*, *Support Vector Machine* (SVM), dan *Deep Neural Network* (DNN). Misalnya,metode *Random Forest* telah mencapai akurasi hingga 95.19% dalam mendeteksi intrusi pada komunikasi GOOSE,sementara pendekatan berbasis DNN menunjukkan hasil yang lebih baik dengan akurasi deteksi hingga 98%.

Pada penelitian [9] mengembangkan teknik deteksi serangan *Man-In-The-Middle* (MITM) berbasis analisis *Address Resolution Protocol* (ARP) untuk meningkatkan keamanan komunikasi antar endpoint. Dari berbagai metode *machine learning* yang digunakan, Linear SVC dan *Gaussian Naive Bayes* memberikan akurasi tertinggi sebesar 99,72%. Penelitian ini merekomendasikan eksplorasi lebih lanjut pada jaringan yang lebih besar dan kompleks untuk meningkatkan ketahanan terhadap serangan canggih.

Penelitian [10] menggunakan metode berbasis *Convolutional Neural Network* (CNN) untuk mendeteksi serangan siber Insider pada sistem otomatisasi substation (SAS). Metode ini mencapai akurasi deteksi sebesar 97,37% dengan waktu pemrosesan 33,786 ms, menunjukkan efisiensi dan efektivitas dalam deteksi serangan waktu nyata. Penelitian ini merekomendasikan penerapan pada sistem

Smart Grid lainnya, pengembangan metode deteksi yang lebih canggih, dan pengujian solusi keamanan untuk meningkatkan ketahanan sistem otomatisasi.

Penelitian [11] mengembangkan sistem deteksi intrusi (IDS) untuk jaringan komunikasi IEC-61850 di stasiun listrik digital untuk mengatasi masalah keamanan baru. Penelitian ini meningkatkan deteksi serangan dengan mengekstraksi dan mengkorelasikan informasi multilayer yang relevan.Metode *Random Forest* memiliki hasil terbaik, dengan presisi 93.33%, recall 98.04%, F1-Score 95.63%, dan akurasi 95.52%. *Random Tree* dan J48 juga memiliki hasil yang baik, dengan F1-Score lebih dari 90%. Studi ini menunjukkan bahwa menambahkan fitur yang lebih kaya secara signifikan meningkatkan kinerja deteksi intrusi dibandingkan dengan menggunakan hanya fitur GOOSE dan SV.

Pada penelitian [12] menceritakan tentang mekanisme deteksi anomali inovatif untuk melindungi lalu lintas jaringan di stasiun pintar yang berbasis IEC 61850 dari serangan siber yang berjenis *SYN Flooding Attack*. Dengan menggunakan *Long Short Term Memory* (LSTM), akurasi deteksi untuk trafik TCP, MMS, dan GOOSE masing-masing mencapai 0,968, 0,973, dan 0,946, masing-masing dengan akurasi rata-rata 0,962,penelitian ini juga mencatat akurasi 0,974, recall 0,886, dan skor F1 0,928. Studi ini mengusulkan pengembangan model deteksi yang lebih cepat dan akurat yang melibatkan protokol SV dan SNTP lainnya. Ketika suara berada di bawah ambang tertentu, detektif tetap beroperasi dengan akurasi di atas 93,47%.

Mengacu kepada penelitian [12] dalam penelitian ini akan menggunakan pendekatan dengan metode *Long Short Term Memory* (LSTM) untuk mendeteksi serangan MITM pada protokol komunikasi GOOSE IEC 61850. LSTM digunakan untuk mempelajari pola perilaku normal dari data lalu lintas jaringan LSTM efektif dalam mengatasi masalah *vanishing gradient* dan mampu mengenali hubungan jangka panjang antar data, yang sangat penting untuk menganalisis data yang berurutan yang tentunya sangat efektif dan relevan dengan penelitian ini.

1.2 Rumusan Masalah

Berdasarkan latar belakang tersebut, maka dapat disimpulkan bahwa rumusan masalah dalam penelitian ini antara lain adalah sebagai berikut:

1. Bagaimana proses pengolahan *dataset* IEC 61850?

2. Bagaimana cara mendeteksi serangan MITM menggunakan algoritma *Long Short Term Memory* (LSTM)?
3. Bagaimana peforma model *Long Short Term Memory* (LSTM) dalam mendeteksi serangan?

1.3 Tujuan

Berdasarkan dari penelitian yang dilakukan maka adapun tujuan dari penelitian ini adalah :

1. Menganalisis dan mengimplementasikan proses pengolahan dataset IEC 61850 agar siap digunakan dalam pemodelan.
2. Mengembangkan model deteksi serangan *Man In The Middle* (MITM) menggunakan algoritma *Long Short Term Memory* (LSTM).
3. Mengevaluasi peforma model LSTM dalam mendeteksi serangan MITM berdasarkan metrik evaluasi yang relevan.

1.4 Manfaat

Adapun manfaat dari penulisan tugas akhir ini, yaitu :

1. Meningkatkan tingkat keamanan komunikasi dalam protokol GOOSE IEC 61850.
2. Menyediakan solusi yang lebih efisien untuk mendeteksi serangan MITM pada sistem tenaga listrik.
3. Memperkenalkan metode *Long Short Term Memory* (LSTM) untuk deteksi serangan, yang dapat meningkatkan ketahanan dan keandalan sistem gardu induk.

1.5 Batasan Masalah

Adapun batasan-batasan masalah dari penyusunan tugas akhir ini, yaitu :

1. Fokus penelitian hanya pada deteksi serangan *Man-In-The-Middle* (MITM) yang terjadi pada protokol GOOSE IEC 61850.
2. Penelitian ini terbatas pada penerapan metode *Long Short Term Memory* (LSTM) dalam deteksi serangan.
3. Fokus penelitian hanya pada jenis serangan MITM, tanpa mencakup jenis serangan lainnya.

1.6 Sistematika penelitian

Penyusunan penelitian ini akan disusun secara sistematis dengan urutan per-bab yang mencakup uraian secara detail dari tiap bab dan sub bab yang relevan. Sistematika penulisan penelitian ini adalah sebagai berikut:

BAB I PENDAHULUAN

Bab ini berisi penjelasan mengenai topik penelitian, yang mencakup latar belakang , rumusan masalah, tujuan penelitian, dan manfaat penelitian.

BAB II TINJAUAN PUSTAKA

Bab ini menguraikan teori-teori dan penelitian terdahulu yang relevan dengan topik penelitian ini. Penjelasan tentang SCADA , protokol GOOSE IEC 61850, ancaman MITM, serta metode deteksi menggunakan LSTM.

BAB III METODOLOGI PENELITIAN

Bab ini menjelaskan secara rinci langkah-langkah penelitian yang dilakukan, termasuk desain eksperimen, pengumpulan data, serta teknik yang digunakan dalam analisis. Di sini juga akan dijelaskan mengenai pendekatan berbasis LSTM yang digunakan untuk mendeteksi serangan MITM, serta algoritma yang diterapkan dalam penelitian ini.*Flowchart* atau diagram blok yang menggambarkan proses metodologi juga akan disajikan.

BAB IV PENGUJIAN DAN ANALISA

Bab ini menguraikan tentang pelaksanaan pengujian serta analisis terhadap hasil pengujian. Penulis akan menjelaskan cara menguji sistem deteksi serangan MITM berbasis LSTM yang dikembangkan, termasuk analisis hasil yang diperoleh dari pengujian tersebut. Dalam bab ini juga akan dijelaskan cara mengukur akurasi deteksi dan tingkat alarm palsu pada sistem yang dikembangkan.

BAB V KESIMPULAN

Bab ini merupakan bab penutup yang berisikan kesimpulan dari penelitian, berdasarkan hasil pengujian dan analisis yang dilakukan. Selain itu, bab ini juga memberikan saran-saran untuk pengembangan lebih lanjut dan penelitian lanjutan dalam meningkatkan deteksi serangan MITM pada protokol GOOSE IEC 61850.

DAFTAR PUSTAKA

[1] M. Boeding, M. Hempel, H. Sharif, J. Lopez, and K. Perumalla, "A flexible OT testbed for evaluating on-device implementations of IEC-61850 GOOSE," *Int. J. Crit. Infrastruct. Prot.*, vol. 42, no. March, p. 100618, 2023, doi: 10.1016/j.ijcip.2023.100618.

[2] J. Suaboot *et al.*, "A Taxonomy of Supervised Learning for IDSs in SCADA Environments To cite this version : HAL Id : hal-02865816 A Taxonomy of Supervised Learning for IDSs in SCADA Environments," 2020.

[3] A. A. Elbaset, Y. S. Mohamed, and A. N. A. Elghaffar, "IEC 61850 communication protocol with the protection and control numerical relays for optimum substation automation system," *J. Eng. Sci. Technol. Rev.*, vol. 13, no. 2, pp. 1–12, 2020, doi: 10.25103/jestr.132.01.

[4] H. T. Reda *et al.*, "Vulnerability and impact analysis of the iec 61850 goose protocol in the smart grid," *Sensors*, vol. 21, no. 4, pp. 1–20, 2021, doi: 10.3390/s21041554.

[5] G. Elbez, K. Nahrstedt, and V. Hagenmeyer, "Early Detection of GOOSE Denial of Service (DoS) Attacks in IEC 61850 Substations," *2022 IEEE Int. Conf. Commun. Control. Comput. Technol. Smart Grids, SmartGridComm 2022*, pp. 367–373, 2022, doi: 10.1109/SmartGridComm52983.2022.9961042.

[6] A. Levchenko and J. Schmalian, "rna lP pro of Jou," *Ann. Phys. (N. Y).*, p. 168218, 2020, doi: 10.1016/j.future.2025.107714.

[7] S. Bhattacharya, N. Saqib, and M. Govindarasu, "ML-based Anomaly Detection System for IEC 61850 Communication in Substations," *IEEE Power Energy Soc. Gen. Meet.*, no. i, pp. 1–5, 2024, doi: 10.1109/PESGM51994.2024.10688773.

[8] H. Nhung-Nguyen, M. Girdhar, Y. H. Kim, and J. Hong, "Machine-Learning-Based Anomaly Detection for GOOSE in Digital Substations," *Energies*, vol. 17, no. 15, pp. 1–20, 2024, doi: 10.3390/en17153745.

[9] J. J. Kponyo, J. O. Agyemang, and G. S. Klogo, "Detecting End-Point (EP) Man-In-The-Middle (MITM) Attack based on ARP Analysis: A Machine Learning Approach," *Int. J. Commun. Networks Inf. Secur.*, vol. 12, no. 3, pp. 384–388, 2020, doi: 10.17762/ijcnis.v12i3.4735.

[10] M. Oinonen and W. G. Morsi, "Real-time detection of insider attacks on substation automation systems using short length orthogonal wavelet filters and OPAL-RT," *Int. J. Electr. Power Energy Syst.*, vol. 162, no. September, p. 110311, 2024, doi: 10.1016/j.ijepes.2024.110311.

[11] V. E. Quincozes, S. E. Quincozes, C. Albuquerque, D. Passos, and D.

Mosse, “Feature Extraction for Intrusion Detection in IEC-61850 Communication Networks,” *2022 6th Cyber Secur. Netw. Conf. CSNet 2022*, pp. 1–7, 2022, doi: 10.1109/CSNet56116.2022.9955599.

[12] L. Yang, Y. Zhai, Y. Zhang, Y. Zhao, Z. Li, and T. Xu, “A new methodology for anomaly detection of attacks in IEC 61850-based substation system,” *J. Inf. Secur. Appl.*, vol. 68, no. July, p. 103262, 2022, doi: 10.1016/j.jisa.2022.103262.

[13] 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.

[14] P. T. C., K. G. Boroojeni, M. Hadi Amini, N. R. Sunitha, and S. S. Iyengar, “Key pre-distribution scheme with join leave support for SCADA systems,” *Int. J. Crit. Infrastruct. Prot.*, vol. 24, pp. 111–125, 2019, doi: 10.1016/j.ijcip.2018.10.011.

[15] 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.

[16] A. Chawla, M. A. Aftab, S. M. S. Hussain, B. K. Panigrahi, and T. S. Ustun, “Cyber–physical testbed for Wide Area Measurement System employing IEC 61850 and IEEE C37.118 based communication,” *Energy Reports*, vol. 8, pp. 570–578, 2022, doi: 10.1016/j.egyr.2022.05.207.

[17] D. Pliatsios, P. Sarigiannidis, T. Lagkas, and A. G. Sarigiannidis, “A Survey on SCADA Systems: Secure Protocols, Incidents, Threats and Tactics,” *IEEE Commun. Surv. Tutorials*, vol. 22, no. 3, pp. 1942–1976, 2020, doi: 10.1109/COMST.2020.2987688.

[18] H. J. S and M. M. Raju, “A Study on Deep Learning,” *Int. J. Res. Appl. Sci. Eng. Technol.*, vol. 10, no. 11, pp. 961–964, 2022, doi: 10.22214/ijraset.2022.47486.

[19] M. Kim, I. Pelivanov, and M. O’Donnell, “Review of Deep Learning Approaches for Interleaved Photoacoustic and Ultrasound (PAUS) Imaging,” *IEEE Trans. Ultrason. Ferroelectr. Freq. Control*, vol. 70, no. 12, pp. 1591–1606, 2023, doi: 10.1109/TUFFC.2023.3329119.

[20] A. M. Musolf, E. R. Holzinger, J. D. Malley, and J. E. Bailey-Wilson, “What makes a good prediction? Feature importance and beginning to open the black box of machine learning in genetics,” *Hum. Genet.*, vol. 141, no. 9, pp. 1515–1528, 2022, doi: 10.1007/s00439-021-02402-z.

[21] B. Lindemann, B. Maschler, N. Sahlab, and M. Weyrich, “A survey on anomaly detection for technical systems using LSTM networks,” *Comput. Ind.*, vol. 131, p. 103498, 2021, doi: 10.1016/j.compind.2021.103498.

[22] K. Adam, K. Smagulova, and A. P. James, “Memristive LSTM network hardware architecture for time-series predictive modeling problems,” *2018*

IEEE Asia Pacific Conf. Circuits Syst. APCCAS 2018, pp. 459–462, 2018, doi: 10.1109/APCCAS.2018.8605649.

[23] O. Surakhi *et al.*, "Time-lag selection for time-series forecasting using neural network and heuristic algorithm," *Electron.*, vol. 10, no. 20, 2021, doi: 10.3390/electronics10202518.

[24] A. A. Hussin Adam Khatir and M. Bee, "Machine Learning Models and Data-Balancing Techniques for Credit Scoring: What Is the Best Combination?," *Risks*, vol. 10, no. 9, 2022, doi: 10.3390/risks10090169.

[25] S. Bagui and K. Li, "Resampling imbalanced data for network intrusion detection datasets," *J. Big Data*, vol. 8, no. 1, 2021, doi: 10.1186/s40537-020-00390-x.

[26] N. García-Pedrajas, "Partial random under/oversampling for multilabel problems," *Knowledge-Based Syst.*, vol. 302, no. July, p. 112355, 2024, doi: 10.1016/j.knosys.2024.112355.

[27] M. Heydarian, T. E. Doyle, and R. Samavi, "MLCM: Multi-Label Confusion Matrix," *IEEE Access*, vol. 10, pp. 19083–19095, 2022, doi: 10.1109/ACCESS.2022.3151048.

[28] J. Xu, Y. Zhang, and D. Miao, "Three-way confusion matrix for classification: A measure driven view," *Inf. Sci. (Ny).*, vol. 507, pp. 772–794, 2020, doi: 10.1016/j.ins.2019.06.064.

[29] M. Owusu-Adjei, J. Ben Hayfron-Acquah, T. Frimpong, and G. Abdul-Salaam, "Imbalanced class distribution and performance evaluation metrics: A systematic review of prediction accuracy for determining model performance in healthcare systems," *PLOS Digit. Heal.*, vol. 2, no. 11 November, pp. 1–23, 2023, doi: 10.1371/journal.pdig.0000290.

[30] P. Fränti and R. Mariescu-Istodor, "Soft precision and recall," *Pattern Recognit. Lett.*, vol. 167, pp. 115–121, 2023, doi: 10.1016/j.patrec.2023.02.005.

[31] E. Dritsas and M. Trigka, "Supervised Machine Learning Models for Liver Disease Risk Prediction," *Computers*, vol. 12, no. 1, p. 19, 2023, doi: 10.3390/computers12010019.

[32] D. Chicco and G. Jurman, "The advantages of the Matthews correlation coefficient (MCC) over F1 score and accuracy in binary classification evaluation," *BMC Genomics*, vol. 21, no. 1, pp. 1–13, 2020, doi: 10.1186/s12864-019-6413-7.