DETEKSI SERANGAN *DENIAL OF SERVICE* (DOS) PADA JARINGAN IEC 61850 *SUPERVISORY CONTROL AND DATA ACQUISITION* (SCADA) MENGGUNAKAN METODE *LONG SHORT-TERM MEMORY* (LSTM)

TUGAS AKHIR

Diajukan Untuk Melengkapi Salah Satu Syarat

Memperoleh Gelar Sarjana Komputer

Oleh :

Muhamad Zaman Rinaldi

09011381924103

JURUSAN SISTEM KOMPUTER

FAKULTAS ILMU KOMPUTER

UNIVERSITAS SRIWIJAYA

2024

LEMBAR PENGESAHAN

DETEKSI SERANGAN *DENIAL OF SERVICE* (DOS) PADA JARINGAN IEC 61850 *SUPERVISORY CONTROL AND DATA ACQUISITION* (SCADA) MENGGUNAKAN METODE *LONG SHORT-TERM MEMORY* (LSTM)

TUGAS AKHIR

Program Studi Sistem Komputer
Jenjang S1

Oleh:

Muhamad Zaman Rinaldi
09011381924103

Palembang, 27 Mei 2024

Mengetahui,
Ketua Jurusan Sistem Komputer

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

Pembimbing Tugas Akhir

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

ii

HALAMAN PERSETUJUAN

Telah diuji dan lulus pada

Hari : Jumat

Tanggal : 17 Mei 2024

Tim Penguji

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

Mengetahui 27/5/24

Ketua Jurusan Sistem Komputer

Dr. Ir. Sukemi, M.T.

NIP. 196612032006041001

iii

HALAMAN PERNYATAAN

Yang bertanda tangan dibawah ini:

Nama	:	Muhamad Zaman Rinaldi
NIM	:	09011381924103
Judul	:	Deteksi Serangan *Denial of Service* (DoS) pada Jaringan IEC 61850 *Supervisory Control and Data Acquisition* (SCADA) menggunakan Metode *Long Short-Term Memory* (LSTM)

Hasil Pengecekan Plagiat/Turnitin: 16%

Menyatakan bahwa laporan tugas akhir ini adalah hasil karya saya sendiri dan tidak mengandung unsur penjiplakan atau plagiat. Saya sepenuhnya menyadari bahwa jika terbukti adanya penjiplakan atau plagiat dalam laporan tugas akhir ini, saya siap menerima sanksi akademik dari Universitas Sriwijaya. Pernyataan ini saya buat dengan kesadaran penuh dan tanpa adanya paksaan dari pihak manapun.

Palembang, 28 Mei 2024

Muhamad Zaman Rinaldi

NIM. 09011381924103

iv

KATA PENGANTAR

Assalamu'alaikum Warahmatullahi Wabarakatuh,

Puji dan syukur penulis panjatkan kepada Allah SWT yang telah melimpahkan rahmat dan karunianya yang sangat besar dan tidak berhenti, sehingga penulis dapat menyelesaikan Tugas Akhir dengan judul **"Deteksi Serangan *Denial of Service* (DoS) pada Jaringan IEC 61850 *Supervisory Control and Data Acquisition* (SCADA) menggunakan Metode *Long Short-Term Memory* (LSTM)"** ini. Shalawat serta salam tak lupa kita curahkan kepada junjungan kita Nabi Muhammad SAW beserta keluarga, sahabat dan para pengikutnya yang insyaallah istiqomah hingga akhir zaman.

Selesainya penyusunan tugas akhir ini tidak terlepas dari peran semua pihak ata ide, bimbingan, dan saran serta bantuannya dalam menyelesaikan penulisan tugas akhir ini, antara lain :

1. Allah SWT yang telah memberikan berkah serta nikmat kesehatan dan kesempatan kepada penulis sehingga dapat menyelesaikan tugas akhir ini.
2. Kepada kedua orang tua yang selalu mendoakan serta memberikan motivasi dan dukungan baik secara moral, material maupun spiritual selama ini.
3. Bapak Prof. Dr. Erwin, S.Si, M.Si. selaku Dekan Fakultas Ilmu Komputer Universitas Sriwijaya dan juga sebagai Dosen Pembimbing Akademik Jurusan Sistem Komputer.
4. Bapak Julian Supardi, S.Pd., M.T. selaku Wakil Dekan Bidang Akademik di Fakultas Ilmu Komputer Universitas Sriwijaya.
5. Bapak Dr. Ir. H. Sukemi, M.T., selaku ketua Jurusan Sistem Komputer Fakultas Ilmu Komputer Universitas Sriwijaya.
6. Bapak Prof. Deris Stiawan, S.Kom., M.T., Ph.D., IPU., ASEAN-Eng. selaku Dosen Pembimbing Tugas Akhir.
7. Ibu Nurul Afifah, M.Kom. selaku dosen Sistem Komputer yang telah membantu dan memberikan masukan selama pengerjaan Tugas Akhir.
8. Bapak dan Ibu dosen jurusan Sistem Komputer yang telah membagikan ilmu dan pengalamannya kepada saya.

9. Mbak Sari Nuzulastri selaku admin Jurusan Sistem Komputer yang telah membantu mengurus seluruh berkas administrasi selama perkuliahan.
10. Teman–teman seperjuangan Jurusan Sistem Komputer Angkatan 2019.
11. Seluruh pihak yang tergabung dalam COMNETS dan CoE terutama Abel, Dendi, Septi, Ageng, Wahyu, Galih, dan Imam yang membantu penulis dalam penelitian ini.
12. Teman–teman saya yang tergabung dalam Grup baCOD Mobile yang selalu memberikan dukungan kepada penulis.
13. Seluruh pihak yang tidak dapat penulis sebutkan satu persatu, yang telah memberikan semangat serta doa.
14. Jurusan Sistem Komputer.
15. Almamater.

Penulis menyadari bahwa dalam penyusunan Tugas Akhir ini masih sangat jauh dari kata sempurna. Oleh karena itu penulis mengharapkan kritik dan saran yang membangun, semoga Tugas Akhir ini dapat bermanfaat dan berguna bagi siapa saja yang membacanya.

Wassalamu'alaikum Warahmatullahi Wabarakatuh.

Palembang, Mei 2024

Penulis,

Muhamad Zaman Rinaldi

NIM. 09011381924103

DETEKSI SERANGAN *DENIAL OF SERVICE* (DOS) PADA JARINGAN IEC 61850 *SUPERVISORY CONTROL AND DATA ACQUISITION* (SCADA) MENGGUNAKAN METODE *LONG SHORT-TERM MEMORY* (LSTM)

MUHAMAD ZAMAN RINALDI (09011381924103)
Jurusan Sistem Komputer, Fakultas Ilmu Komputer
Universitas Sriwijaya
Email : zamanrinaldi@gmail.com

ABSTRAK

Supervisory Control and Data Acquisition (SCADA) banyak digunakan dalam industri sebagai sebuah sistem yang bertugas untuk mengawasi, mengendalikan dan secara bersamaan dapat mengumpulkan data dari sensor yang dihubungkan selama proses produksi berjalan. SCADA memiliki sebuah protokol IEC 61850 GOOSE yang digunakan sebagai jalur komunikasi antar *Intelligent Electronic Device* (IED). Jalur komunikasi ini dapat dilakukan injeksi untuk mengirimkan paket yang memiliki *status number* (StNum) yang tidak normal dengan jumlah yang banyak dan dalam waktu singkat untuk melakukan serangan *Denial of Service* (DoS) yang mengakibatkan IED tidak dapat berfungsi seperti semestinya. Penelitian ini menggunakan algoritma *Long Short-Term Memory* (LSTM) untuk mendeteksi pola serangan DoS dalam dataset. Dataset yang digunakan berasal dari *IEC61850SecurityDataset* yang berisi data protokol GOOSE pada jaringan SCADA yang sudah terinjeksi DoS. Dikarenakan distribusi datanya yang tidak seimbang dataset tersebut diseimbangkan menggunakan *random oversampling*. Model terbaik dari penelitian ini mencapai tingkat akurasi sebesar 98,24%, dengan *precision* 100%, *recall* 92,22%, dan F1 *score* 98,22%.

Kata Kunci : *Supervisory Control and Data Acquisition*, *Denial of Service, IEC 61850, Long Short-Term Memory*

DENIAL OF SERVICE (DOS) ATTACK DETECTION ON IEC 61850 SUPERVISORY CONTROL AND DATA ACQUISITION (SCADA) NETWORK USING LONG SHORT-TERM MEMORY (LSTM)

MUHAMAD ZAMAN RINALDI (09011381924103)

Computer Engineering Department, Computer Science Faculty

Sriwijaya University

Email : zamanrinaldi@gmail.com

ABSTRACT

Supervisory Control and Data Acquisition (SCADA) is widely used in industry as a system that is tasked with supervising, controlling while simultaneously collecting data from sensors connected during the production process. SCADA has an IEC 61850 GOOSE protocol which is used as a communication line between Intelligent Electronic Device (IED). This communication line can be injected to send packets that have an abnormal status number (StNum) on a large amount and in a short period of time to carry out a Denial of Service (DoS) attack which results in the IED not being able to function properly. This research uses the Long Short-Term Memory (LSTM) algorithm to detect DoS attack patterns in the dataset. The dataset used is from IEC61850SecurityDataset which contains GOOSE protocol data on SCADA networks that have been injected with DoS. Due to the unbalanced data distribution the dataset was balanced using random oversampling. The best model from this study achieved an accuracy rate of 98.24%, with precision 100%, recall 92.22%, and F1 score 98.22%.

Keywords *: Supervisory Control and Data Acquisition, Denial of Service, IEC 61850, Long Short-Term Memory*

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

BAB I
PENDAHULUAN

1.1 Latar Belakang

Supervisory Control and Data Acquisition (SCADA) banyak digunakan dalam industri sebagai sebuah sistem yang bertugas untuk mengawasi, mengendalikan dan secara bersamaan dapat mengumpulkan data dari sensor yang dihubungkan selama proses produksi berjalan. Ratusan maupun ribuan data tersebut akan dianalisis dan mengirimkan status dari setiap bagian perangkat pada lapangan ke *Master Terminal Unit* (MTU) sehingga user yang mengendalikan dapat mengetahui apabila terjadinya gangguan, user juga dapat mengirimkan perintah ke setiap perangkat yang ada dalam proses produksi tersebut[1].

SCADA memiliki sebuah protokol IEC 61850 GOOSE yang digunakan sebagai jalur komunikasi antar *Intelligent Electronic Device* (IED) agar bisa saling mengirimkan informasi mengenai status dari IED tersebut, sehingga apabila terjadi kerusakan diantaranya akan didukung oleh bagian lainnya[2]. Berdasarkan hal tersebut, tidak menutup kemungkinan terjadi serangan yang akan menimbulkan masalah kedepannya.

Denial of Service (DoS) merupakan serangan yang dapat terjadi apabila sebuah sistem dibanjiri dengan permintaan yang berlebihan sehingga sistem terbebani dan tidak dapat melakukan permintaan yang semestinya[3]. Pada penelitian sebelumnya [4] disebutkan bahwa dalam jaringan SCADA, terutama pada protokol GOOSE sendiri DoS dapat dilakukan dengan mengirimkan paket yang memiliki *status number* (StNum) yang tidak normal dengan jumlah yang banyak dalam waktu singkat sehingga dapat menyebabkan IED tidak dapat berfungsi seperti semestinya.

Pada penelitian tugas akhir skripsi ini penulis akan berfokus pada serangan *Denial of Service* (DoS) pada jaringan SCADA protokol IEC 61850 GOOSE yang akan dideteksi menggunakan algoritma Deep Learning yaitu *Long Short-Term Memory* (LSTM). LSTM sendiri adalah algoritma *Deep Learning* yang merupakan turunan dari *Recurrent Neural Network* (RNN) yang diperkenalkan pada tahun 1997 oleh Hochreiter dan Schmidhuber. LSTM dapat menggunakan ingatan

panjang sebagai input dari fungsi aktivasi dalam lapisan tersembunyi (*hidden layer*). Metode ini biasa digunakan untuk memprediksi sekaligus mengklasifikasikan data berdasarkan urutan waktu tertentu (*time-series*) [5][6].

Pada penelitian [7] yang melakukan survey terhadap deteksi anomali menggunakan jaringan LSTM menyebutkan bahwa jaringan LSTM sangat cocok digunakan untuk data dengan rangkaian waktu (*time series*) yang dimana digunakan pada penelitian ini.

Berdasarkan ulasan diatas maka penulis mengusulkan untuk melakukan penelitian dengan judul *"Deteksi Serangan Denial Of Service (DoS) Pada Jaringan IEC 61850 Supervisory Control and Data Acquisition (SCADA) Menggunakan Metode Long Short-Term Memory (LSTM)"*.

1.2 Rumusan Masalah

Adapun rumusan masalah dari penelitian ini, yakni :

1. Bagaimana cara membedakan data serangan dan data normal?
2. Bagaimana cara yang dapat dilakukan untuk mengatasi data yang tidak seimbang agar dapat mencapai kinerja optimal?
3. Bagaimana cara mendeteksi serangan *Denial of Service* (DoS) pada dataset yang digunakan?

1.3 Batasan Masalah

Adapun batasan masalah dalam penelitian ini adalah :

1. Menggunakan dataset *IEC61850SecurityDataset* pada tahun 2019.
2. Dataset yang digunakan memiliki distribusi yang tidak seimbang antara data serangan dan data normal.
3. Menggunakan algoritma *Long Short-Term Memory* (LSTM) untuk mendeteksi adanya serangan *Denial of Service* (DoS) pada data tersebut.

1.4 Tujuan Penelitian

Berdasarkan perumusan masalah yang telah ditentukan, maka dibentuk juga tujuan dari penelitian ini, yaitu :

1. Membedakan data serangan dengan data normal pada dataset.

2. Menyeimbangkan distribusi dataset dengan menggunakan metode *oversampling*.
3. Mendeteksi adanya serangan *Denial of Service* (DoS) pada dataset.

1.5 Manfaat Penelitian

Adapun manfaat dari penelitian ini yaitu :

1. Dapat membedakan data serangan dengan data normal pada dataset.
2. Dapat menyeimbangkan distribusi dataset dengan menggunakan metode *oversampling*.
3. Dapat mendeteksi adanya serangan *Denial of Service* (DoS) pada dataset.

1.6 Metodologi Penelitian

Metodologi yang dilakukan oleh penulis dalam penelitian ini yaitu :

1.6.1 Metode Studi Pustaka dan Literatur

Pada metode ini penulis melakukan pengumpulan beberapa referensi berupa literatur ilmiah yang terdapat pada buku, jurnal, maupun artikel yang berhubungan dengan penelitian yang dilakukan.

1.6.2 Metode Konsultasi

Pada metode ini penulis melakukan konsultasi secara langsung dan atau tidak langsung kepada pihak narasumber yang memiliki pengetahuan serta wawasan yang baik dalam mengatasi permasalahan yang ditemui pada penelitian yang sedang dilakukan.

1.6.3 Metode Pengolahan Data

Pada metode ini penulis melakukan ekstraksi fitur dari data PCAP yang digunakan dalam penelitian menjadi bentuk CSV serta melakukan seleksi fitur sesuai dengan pola serangan yang akan dideteksi.

1.6.4 Metode Pembuatan Model dan Pengujian Data

Pada metode ini penulis membuat perancangan pemodelan pada dataset yang telah diolah pada tahap sebelumnya menggunakan *Deep Learning* untuk mendapatkan akurasi yang diinginkan.

1.6.5 Metode Analisis dan Kesimpulan

Pada tahap ini penulis melakukan analisa serta membuat kesimpulan dan saran berdasarkan hasil dari penelitian yang telah dikerjakan sehingga dapat digunakan sebagai referensi untuk penelitian yang akan datang.

1.7 Sistematika Penulisan

Adapun sistematika dalam penulisan Tugas Akhir ini sebagai berikut :

BAB I PENDAHULUAN

BAB I memberikan penjelasan mengenai latar belakang, tujuan, manfaat, perumusan masalah, batasan masalah, metodologi penelitian, dan sistematika penulisan pada penulisan tugas akhir ini.

BAB II TINJAUAN PUSTAKA

BAB II mengandung literature review dari penelitian dan teori terkait yang dijadikan acuan serta pendukung penelitian ini yang diantaranya *Supervisory Control and Data Acquisition* (SCADA), protokol IEC 61850, *Denial of Service* (DoS), *Deep Learning*, dan metode *Long Short-Term Memory* (LSTM).

BAB III METODOLOGI PENELITIAN

BAB III berisi penjelasan mengenai proses penelitian, kerangka kerja, serta perancangan dari model *Long Short-Term Memory* (LSTM) yang digunakan pada penelitian dalam mendeteksi serangan *Denial of Service* (DoS).

BAB IV HASIL DAN ANALISA

BAB IV akan menjelaskan hasil dari penelitian yang dilakukan, serta melakukan analisis dari Deteksi Serangan *Denial Of Service* (DoS) Pada Jaringan IEC 61850 *Supervisory Control And Data Acquisition* (SCADA) Menggunakan Metode *Long Short-Term Memory* (LSTM).

BAB V KESIMPULAN DAN SARAN

BAB V berisi kesimpulan dari penelitian yang telah dilakukan dan juga saran agar dapat dikembangkan kembali pada penelitian selanjutnya.

DAFTAR PUSTAKA

[1] 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.

[2] P. P. Biswas, H. C. Tan, Q. Zhu, Y. Li, D. Mashima, and B. Chen, "A synthesized dataset for cybersecurity study of IEC 61850 based substation," *2019 IEEE Int. Conf. Commun. Control. Comput. Technol. Smart Grids, SmartGridComm 2019*, pp. 1–7, 2019, doi: 10.1109/SmartGridComm.2019.8909783.

[3] J. Gao *et al.*, "Omni SCADA Intrusion Detection Using Deep Learning Algorithms," *IEEE Internet Things J.*, vol. 8, no. 2, pp. 951–961, 2021, doi: 10.1109/JIOT.2020.3009180.

[4] 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.

[5] N. K. Manaswi, *Deep Learning with Applications Using Python*. 2018. doi: 10.1007/978-1-4842-3516-4.

[6] A. Chamekh, M. Mahfoudh, and G. Forestier, "Sentiment Analysis Based on Deep Learning in E-Commerce," *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 13369 LNAI, pp. 498–507, 2022, doi: 10.1007/978-3-031-10986-7_40.

[7] 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.

[8] 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.

[9] P. I. Radoglou-Grammatikis and P. G. Sarigiannidis, "Securing the Smart Grid: A Comprehensive Compilation of Intrusion Detection and Prevention Systems," *IEEE Access*, vol. 7, pp. 46595–46620, 2019, doi: 10.1109/ACCESS.2019.2909807.

[10] 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.

[11] P. P. Shinde and S. Shah, "A Review of Machine Learning and Deep Learning Applications," *Proc. - 2018 4th Int. Conf. Comput. Commun. Control Autom. ICCUBEA 2018*, pp. 1–6, 2018, doi: 10.1109/ICCUBEA.2018.8697857.

[12] 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.

[13] T. R. Shultz and S. E. Fahlman, *Encyclopedia of Machine Learning and Data Mining*. 2017. doi: 10.1007/978-1-4899-7687-1.

[14] R. Susmaga, "Confusion Matrix Visualization," *Intell. Inf. Process. Web Min.*, pp. 107–116, 2004, doi: 10.1007/978-3-540-39985-8_12.

[15] 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.

[16] 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.

[17] M. Mimura, "Impact of benign sample size on binary classification accuracy,"

Expert Syst. Appl., vol. 211, no. November 2021, p. 118630, 2023, doi: 10.1016/j.eswa.2022.118630.

[18] E. Ropelewska, V. Slavova, K. Sabanci, M. Fatih Aslan, X. Cai, and S. Genova, "Discrimination of onion subjected to drought and normal watering mode based on fluorescence spectroscopic data," *Comput. Electron. Agric.*, vol. 196, no. March, p. 106916, 2022, doi: 10.1016/j.compag.2022.106916.

[19] Z. Meng, H. Huo, Z. Pan, L. Cao, J. Li, and F. Fan, "A gear fault diagnosis method based on improved accommodative random weighting algorithm and BB-1D-TP," *Meas. J. Int. Meas. Confed.*, vol. 195, no. March, p. 111169, 2022, doi: 10.1016/j.measurement.2022.111169.

[20] M. Boubaris, A. Cameron, J. Manakil, and R. George, "Artificial intelligence vs . semi-automated segmentation for assessment of dental periapical lesion volume index score : A cone-beam CT study," *Comput. Biol. Med.*, vol. 175, no. April, p. 108527, 2024, doi: 10.1016/j.compbiomed.2024.108527.