DETEKSI SERANGAN *MAN IN THE MIDDLE* (MITM) PADA PROTOKOL JARINGAN IEC 61850 *SUPERVISORY CONTROL AND DATA ACQUISITION* (SCADA) DENGAN MENGGUNAKAN METODE *DECISION TREE*

TUGAS AKHIR

Diajukan Untuk Melengkapi Salah Satu Syarat

Memperoleh Gelar Sarjana Komputer

Oleh:

Muhammad Syahrul Wijaya

09011282126085

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 *DECISION TREE*

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

Oleh:

MUHAMMAD SYAHRUL WIJAYA
09011282126085

Pembimbing 1	**: Prof. Ir. Deris Stiawan, M.T., Ph.D.**
	NIP. 197806172006041002
Pembimbing 2	**: Nurul Afifah, M.Kom.**
	NIP. 199211102023212049

Mengetahui
Ketua Jurusan Sistem Komputer

Dr. Ir. Sukemi, M.T.
196612032006041001

HALAMAN PERSETUJUAN

Telah diuji dan lulus pada

Hari : Jum'at

Tanggal : 13 Juni 2025

Tim Penguji

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

Mengetahui 11/7 '25

Ketua Jurusan Sistem Komputer

Dr. Ir. Sukemi, M.T.

NIP. 196612032006041001

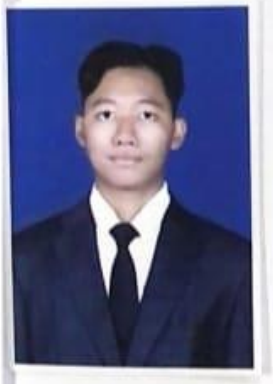
HALAMAN PERNYATAAN

Yang bertanda tangan dibawah ini:

Nama	:	Muhammad Syahrul Wijaya
Nim	:	09011282126085
Judul	:	Deteksi Serangan *Man In The Middle* (MITM) Pada Protokol Jaringan IEC 61850 *Supervisory Control And Data Acquisition* (SCADA) Dengan Menggunakan Metode *Decision Tree*

Hasil Pengecekan Plagiat/Turnitin: 9%

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, Juli 2025

Muhammad Syahrul Wijaya
NIM. 09011282126085

KATA PENGANTAR

Segala puji dan syukur penulis panjatkan ke hadirat Allah SWT atas limpahan rahmat dan karunia-Nya, sehingga penulis dapat menyelesaikan tugas akhir ini dengan judul "Deteksi Serangan *Man In The Middle* (MiTM) Pada Protokol Jaringan IEC 61850 *Supervisory Control And Data Acquisition* (SCADA) Dengan Menggunakan Metode *Decision Tree*". Shalawat serta salam senantiasa tercurah kepada junjungan kita, Nabi Muhammad SAW, beserta keluarga, sahabat, dan para pengikutnya yang istiqomah hingga akhir zaman.

Tugas akhir ini dapat diselesaikan berkat bantuan, bimbingan, dan dukungan dari berbagai pihak. Oleh karena itu, penulis menyampaikan rasa terima kasih yang sebesar-besarnya kepada:

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.
3. Bapak Dr. Ir. H. Sukemi, M.T. selaku Ketua Jurusan Sistem Komputer Fakultas Ilmu Komputer Universitas Sriwijaya.
4. Bapak Huda Ubaya, M.T. selaku Sekretaris Jurusan Sistem Komputer Universitas Sriwijaya.
5. Bapak Iman Saladin B. Azhar, S.Kom., M.MSI., selaku Dosen Pembimbing Akademik.
6. Bapak Prof. Ir. Deris Stiawan, M.T., Ph.D., selaku Dosen Pembimbing 1 dan Ibu Nurul Afifah, M.Kom. selaku Dosen Pembimbing 2 Tugas Akhir, yang telah dengan penuh perhatian meluangkan waktu dan tenaga untuk membimbing, memberikan saran, serta memberikan motivasi kepada penulis sepanjang proses penulisan Tugas Akhir ini.
7. Admin Jurusan Sistem Komputer yang telah membantu penulis dalam hal administrasi selama perkuliahan.
8. Bapak, Ibu dosen jurusan Sistem Komputer yang telah memberikan ilmunya serta pengalamannya kepada penulis.

9. Meta Nur.H selaku teman dan partner yang selalu ada selama proses penyusunan skripsi ini, senantiasa menemani, memberikan semangat, dukungan, doa dan motivasi tambahan yang membantu dalam menyelesaikan tugas akhir ini dengan tepat waktu.
10. Teman–teman saya yang tergabung dalam Grup KAPE TerOP yang selalu memberikan dukungan kepada penulis.
11. Seluruh pihak yang tidak dapat penulis sebutkan satu persatu, yang telah memberikan semangat serta doa.
12. Jurusan Sistem Komputer.
13. Alamamater.

Penulis menyadari bahwa kesempurnaan hanya milik Allah SWT, dan kesalahan maupun kekhilafan adalah bagian dari manusia, termasuk dalam penyusunan tugas akhir ini. Oleh karena itu, penulis dengan rendah hati memohon kritik dan saran yang membangun agar tulisan ini dapat diperbaiki di masa yang akan datang. Penulis juga berharap tugas akhir ini dapat bermanfaat bagi semua pihak yang membacanya dan memberikan kontribusi yang berarti bagi pengembangan ilmu pengetahuan.

Palembang, Juli 2025

Muhammad Syahrul Wijaya
NIM. 09011282126085

DETEKSI SERANGAN *MAN IN THE MIDDLE* (MITM) PADA PROTOKOL JARINGAN IEC 61850 *SUPERVISORY CONTROL AND DATA ACQUISITION* (SCADA) DENGAN MENGGUNAKAN METODE *DECISION TREE*

MUHAMMAD SYAHRUL WIJAYA (09011282126085)
Jurusan Sistem Komputer, Fakultas Ilmu Komputer
Universitas Sriwijaya
Email: syahrulw353@gmail.com

ABSTRAK

International Electrotechnical Commission (IEC) 61850 adalah standar komunikasi yang dirancang khusus untuk otomatisasi gardu listrik, yang memfasilitasi interoperabilitas di antara *Intelligent Electronic Devices* (IEDs) dalam sistem SCADA. Protokol ini mengatasi keterbatasan sistem lama dengan memanfaatkan komunikasi berbasis IP, yang memungkinkan penanganan data yang lebih efisien dan fleksibel. Protokol komunikasi ini rentan terhadap serangan *Man in The Middle* (MiTM), yang dapat menyebabkan APPID pada paket yang dikirimkan dari IEC 61850 berbeda dengan yang seharusnya. Hal ini dapat menyebabkan gangguan pada komunikasi perangkat IED. Pada penelitian ini algoritma yang digunakan adalah *Decision Tree* dengan data tabular yang dilakukan pra-pemrosesan terlebih dahulu sebelum akan digunakan untuk membangun model *Decision Tree*. Model menunjukkan hasil yang memuaskan ada pada perbandingan data 80:20, dengan akurasi 94.43%, *F1-Score* 96.14%, *Recall* 100% dan *Precision* 92.56%.

Kata Kunci : *Supervisory Control and Data Acquisition, Man in The Middle*, IEC 61850, *Decision Tree*

MAN IN THE MIDDLE (MITM) ATTACK DETECTION ON IEC 61850 SUPERVISORY CONTROL AND DATA ACQUISITION (SCADA) NETWORK PROTOCOL USING DECISION TREE

MUHAMMAD SYAHRUL WIJAYA (09011282126085)
Computer Engineering Department, Computer Science Faculty
Sriwijaya University
Email: syahrulw353@gmail.com

ABSTRACT

International Electrotechnical Commission (IEC) 61850 is a communications standard designed specifically for electrical substation automation, facilitating interoperability among Intelligent Electronic Devices (IEDs) in SCADA systems. This protocol overcomes the limitations of legacy systems by utilizing IP-based communications, which allows for more efficient and flexible data handling. This communication protocol is vulnerable to Man in The Middle (MiTM) attacks, which can cause the APPID on packets sent from IEC 61850 to be different from what it should be. This can cause interference with IED device communications. In this research, the algorithm used is a Decision Tree with tabular data which is pre-processed before it is used to build a Decision Tree model. The model shows satisfactory results in a data ratio of 70:30, with an accuracy of 94.43%, F1-Score 96.14%, Recall 100% and Precision 92.56%.

Keywords : *Supervisory Control and Data Acquisition, Man in The Middle,* IEC 61850, *Decision Tree*

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

BAB I
PENDAHULUAN

1.1 Latar Belakang

Sistem *Supervisory Control and Data Acquisition* (SCADA) merupakan komponen pemantauan dan kontrol dan komunikasi *real-time*, yang memastikan kinerja optimal dan pemanfaatan sumber daya yang efisien [1] [2] untuk mendasari infrastruktur penting, seperti tenaga listrik, telekomunikasi, transportasi, jaringan pipa, bahan kimia, dan pabrik manufaktur. Sistem SCADA lama beroperasi pada jaringan yang terisolasi, sehingga tidak terlalu rentan terhadap ancaman Internet. Namun, semakin meningkatnya koneksi sistem SCADA ke Internet, serta jaringan perusahaan, menimbulkan masalah keamanan yang serius. Pertimbangan keamanan untuk sistem SCADA semakin diperhatikan, karena jumlah insiden keamanan terhadap infrastruktur penting ini semakin meningkat [3].

Dalam sistem pembangkit listrik, sistem SCADA menggunakan protokol IEC 61850 sebagai standar komunikasi untuk otomatisasi dan proteksi di pembangkit listrik serta gardu induk [4]. Protokol ini mendukung berbagai jenis komunikasi untuk memastikan interoperabilitas, efisiensi data, dan kecepatan respons. Protokol utama dalam IEC 61850 mencakup GOOSE (*Generic Object-Oriented Substation Event*), yang memungkinkan pengiriman data berbasis peristiwa dengan latensi rendah, ideal untuk komunikasi antar perangkat dalam skenario kritis seperti proteksi relai. Selain itu, terdapat *Sampled Values* (SV) untuk mentransfer data pengukuran analog seperti tegangan dan arus dalam bentuk digital secara sinkron dengan kecepatan tinggi [5]. Protokol MMS (*Manufacturing Message Specification*) digunakan untuk komunikasi *client-server* berbasis TCP/IP, memungkinkan pertukaran informasi seperti konfigurasi, data *real-time*, dan status operasional perangkat [6]. Dengan protokol-protokol ini, IEC 61850 menyediakan kerangka kerja komprehensif untuk pengelolaan, pengendalian, dan proteksi sistem tenaga listrik modern, sekaligus mendukung integrasi teknologi baru. Namun demikian, masih terdapat kekurangan dalam aspek keamanan, terutama terhadap serangan *Man in The Middle* (MITM) dan *Denial of Service* (DoS) karena

kurangnya mekanisme enkripsi [7] [8] dan autentikasi yang kuat dalam protokol seperti GOOSE dan SV, yang dapat dimanipulasi oleh pihak tidak berwenang [2].

Protokol IEC 61850 rentan terhadap berbagai serangan siber, termasuk *Denial of Service* (DoS) dan *Man in The Middle* (MiTM). Dalam serangan DoS, penyerang dapat mengirimkan sejumlah besar pesan GOOSE palsu ke jaringan untuk membanjiri bandwidth dan sumber daya perangkat penerima, menyebabkan keterlambatan atau bahkan kegagalan komunikasi antar perangkat proteksi. Akibatnya, sistem proteksi seperti relai tidak dapat merespons kejadian nyata secara tepat waktu, yang dapat mengganggu stabilitas sistem tenaga listrik. Sementara itu, dalam serangan MITM, penyerang menyisipkan pesan GOOSE palsu ke dalam jaringan tanpa harus mencegat komunikasi asli [7] . Dengan mengeksploitasi kurangnya mekanisme autentikasi dan enkripsi pada GOOSE, penyerang dapat menginjeksi data yang menginstruksikan perangkat proteksi untuk bertindak secara tidak semestinya, seperti memutus aliran listrik atau menunda respons terhadap gangguan [8]. Serangan ini dapat menyebabkan ketidakstabilan sistem atau bahkan pemadaman listrik jika tidak terdeteksi dengan cepat.

Salah satu cara untuk mencegahnya dapat dilakukan pendekatan *machine learning* seperti *Decision Tree* yang dapat menjadi strategi untuk memperkuat keamanan pada protokol IEC 61850 dengan memodelkan perilaku serangan berbasis GOOSE. *Decision tree* merupakan model prediktif yang menghubungkan observasi suatu objek dengan kesimpulan mengenai nilai variabel target. *Decision tree* menyusun diagram konstruksi logis yang mirip dengan sistem berbasis aturan, namun kondisi spesifik untuk mencapai kesimpulan tersebut disajikan secara struktural. Teknik ini sangat dihargai karena kemampuannya menghasilkan model yang mudah dipahami dan dapat diterapkan pada data dalam jumlah besar [9]. Berdasarkan penjelasan diatas maka penulis ingin mengangkat judul "Deteksi Serangan *Man In The Middle* (MiTM) Pada Protokol Jaringan IEC 61850 *Supervisory Control And Data Acquisition* (SCADA) Dengan Menggunakan Metode *Decision Tree*". Diharapkan hasil dari penelitian ini untuk dapat meningkatkan keamanan protokol IEC 61850 dari serangan MiTM.

Pada penelitian [8], Mereka menggunakan metode *Decision Tree* untuk mendeteksi serangan MiTM, kemudian membandingkannya dengan metode lain

seperti *Random Forest, Support Vector Machine, K-Nearest Neighbour* . Dari hasil perbandingan tersebut diketahui bahwa metode *Decision Tree* sangat unggul dalam *detection rate* dan mendapatkan akurasi yang cukup tinggi dibandingkan dengan metode lainnya tersebut.

Pada penelitian [7], Mereka melakukan deteksi dan klasifikasi serangan siber pada *Substation Automation Systems* (SAS). Pada penelitian tersebut mereka menggunakan beberapa metode seperti, *Decision Tree, Convolutional Neural Network, K-Nearest Neighbor, Support Vector Machine*, dan *Random Forest*. Berdasarkan penelitian tersebut, diketahui bahwa metode *Decision Tree* cukup unggul dengan akurasi sebesar 88.16%.

Pada riset [10] untuk mendeteksi serangan pada protokol IEC 61850 menggunakan *machine learning*. Mereka melakukan riset menggunakan metode *Decision Tree* dan juga metode *Support Vector Machine*. Berdasarkan hasil riset tersebut didapatkanlah bahwa metode *Decision Tree* menghasilkan akurasi yang sangat memuaskan yaitu 99,99%.

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 pada dataset IEC 61850 dilakukan?
2. Bagaimana cara mendeteksi serangan MiTM pada dataset IEC 61850 menggunakan algoritma *Decision Tree*?
3. Bagaimana performa model *Decision Tree* dalam mendeteksi serangan *Man in The Middle* (MiTM) pada dataset IEC 61850?

1.3 Batasan Masalah

Adapun batasan masalah dalam penelitian ini antara lain:

1. Fokus pada *dataset* yang digunakan berupa *dataset* SCADA IEC 61850
2. Penelitian ini menggunakan algoritma *Decision Tree* untuk mendeteksi adanya serangan *Man in The Middle* (MiTM) pada *dataset* IEC 61850.
3. Serangan MiTM yang dibahas adalah GOOSE *Spoofing.*

1.4 Tujuan

Berikut ini merupakan tujuan penelitian yang ingin dicapai berdasarkan perumusan masalah yang telah ditentukan, yaitu:

1. Menentukan bagaimana cara pengolahan pada dataset IEC 61850.
2. Mendeteksi adanya serangan MiTM pada perangkat IEC 61850.
3. Mengetahui performa dari model deteksi dengan metode *decision tree* yang dibangun.

1.5 Manfaat

Adapun manfaat yang ingin dicapai dalam penelitian ini adalah sebagai berikut.

1. Dapat melakukan proses pengolahan dengan menggunakan dataset IEC 61850.
2. Dapat mendeteksi adanya paket normal dan paket serangan pada *dataset* IEC 61850 menggunakan metode *decision tree.*
3. Dapat mengetahui hasil performa dari model *decision tree* yang digunakan untuk mendeteksi serangan *Man in The Middle*.

1.6 Metodologi Penelitian

Adapun metodologi penelitian yang digunakan untuk penelitian berjudul "Deteksi Serangan *Man in The Middle* (MiTM) pada protokol jaringan IEC 61850 *Supervisory Control and Data Acquisition* (SCADA) menggunakan metode *Decision Tree*" adalah sebagai berikut.

1. Studi Pustaka dan Literatur

   Metode ini memungkinkan penulis untuk melakukan proses eksplorasi dan pengumpulan referensi dari berbagai sumber, seperti jurnal, artikel, buku, maupun literatur ilmiah lainnya yang relevan dengan penelitian atau riset tugas akhir yang dilakukan.

2. Metode Konsultasi

   Metode ini memungkinkan penulis untuk berkonsultasi, baik secara langsung maupun online, dengan narasumber yang memiliki pengetahuan dan wawasan luas tentang masalah yang dibahas dalam penelitian. Konsultasi ini

bertujuan untuk mendapatkan pemahaman yang lebih baik serta solusi atas permasalahan yang ditemui selama proses riset.

3. Metode Pengolahan Data

   Metode ini memungkinkan penulis untuk mengekstrak fitur dari data PCAP yang digunakan dalam penelitian ke dalam format CSV, kemudian dilakukan seleksi fitur berdasarkan pola serangan yang akan diidentifikasi dan dideteksi.

4. Metode Pengerjaan Model dan Pengujian Data

   Metode ini digunakan oleh penulis untuk merancang model pada dataset yang telah diolah pada tahap sebelumnya menggunakan *machine learning*, dengan tujuan mencapai akurasi yang diharapkan.

5. Metode Analisis dan Kesimpulan

   Pada tahap ini, penulis melakukan analisis, menyusun kesimpulan, dan memberikan saran berdasarkan hasil penelitian yang telah dilakukan, sehingga dapat digunakan sebagai referensi atau acuan untuk penelitian di masa mendatang.

1.7 Sistematika Penulisan

Adapun sistematika pada penulisan tugas akhir ini adalah 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 tentang penelitian sebelumnya dan teori yang relevan untuk mendukung penelitian ini. Teori–teori tersebut termasuk tersebut termasuk *supervisory control and data acquisition* (SCADA), *Man in The Middle* (MiTM), protocol IEC 61850, *machine learning dan Decision Tree*.

BAB III METODOLOGI PENELITIAN

BAB III berisi penjelasan mengenai proses penelitian, kerangka kerja, serta perancangan dari model *Decision Tree* yang digunakan pada penelitian dalam mendeteksi serangan *Man in The Middle* (MiTM).

BAB IV HASIL DAN ANALISA

BAB IV akan menjelaskan hasil dari penelitian yang dilakukan, serta melakukan analisis dari Deteksi Serangan *Man in The Middle* (MiTM) Pada Jaringan IEC 61850 *Supervisory Control And Data Acquisition* (SCADA) Menggunakan Metode *Decision Tree*.

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] G. S. Gnana, A. Karthikeyan, K. Karthikeyan, P. Sanjeevikumar, S. Karapparambil Thomas, and A. Babu, "Critical review Of SCADA And PLC in smart buildings and energy sector," *Energy Reports*, vol. 12, no. March, pp. 1518–1530, 2024, doi: 10.1016/j.egyr.2024.07.041.

[2] B. Hasan, Mohammad Kamrul; Habib, A.K.M. Ahasan; Islam, Shayla; Safie, Nurhizam; Abdullah, Siti Noral Huda Sheikh; Pandey, "DDoS: Distributed denial of service attack in communication standard vulnerabilities in smart grid applications and cyber security with recent developments," *Energy Reports*, vol. 9, pp. 1318–1326, 2023, [Online]. Available: https://doi.org/10.1016/j.egyr.2023.05.184

[3] 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.

[4] E. Holasova, P. Blazek, R. Fujdiak, J. Masek, and J. Misurec, "Exploring the power of convolutional neural networks for encrypted industrial protocols recognition," *Sustain. Energy, Grids Networks*, vol. 38, no. January, p. 101269, 2024, doi: 10.1016/j.segan.2023.101269.

[5] M. Pashaei, H. Rastegar, S. F. Zandrazavi, K. Kauhaniemi, and H. Laaksonen, "Real-time hardware-in-the-loop approach for adaptive centralized protection schemes using clustering algorithms," *Expert Syst. Appl.*, vol. 255, no. PC, p. 124707, 2024, doi: 10.1016/j.eswa.2024.124707.

[6] 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.

[7] 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, 2024, doi: 10.1016/j.ijepes.2024.110311.

[8] T. S. Ustun, *Adaptive protection system for microgrids with high penetration of renewables: IEC 61850 modeling and cybersecurity considerations*. Koriyama, Japan, 2024. [Online]. Available: https://doi.org/10.1016/B978-0-323-91780-3.00006-4

[9] N. D. Barbosa Castro, F. Sáenz Blanco, F. Zorrilla Briones, and E. F. Tapias Forero, "Determination of key resource variables for a model of technological capability management in the alternative electricity generation industry of Colombia and Mexico, through a decision tree," *Heliyon*, vol. 10, no. 22, 2024, doi: 10.1016/j.heliyon.2024.e40448.

[10] H. Lahza, K. Radke, and E. Foo, "Applying domain-specific knowledge to

construct features for detecting distributed denial-of-service attacks on the GOOSE and MMS protocols," *Int. J. Crit. Infrastruct. Prot.*, vol. 20, pp. 48–67, 2018, doi: 10.1016/j.ijcip.2017.12.002.

[11] D. Upadhyay, J. Manero, M. Zaman, and S. Sampalli, "Intrusion Detection in SCADA Based Power Grids: Recursive Feature Elimination Model with Majority Vote Ensemble Algorithm," *IEEE Trans. Netw. Sci. Eng.*, vol. 8, no. 3, pp. 2559–2574, 2021, doi: 10.1109/TNSE.2021.3099371.

[12] C. Y. Lin and S. Nadjm-Tehrani, "Protocol study and anomaly detection for server-driven traffic in SCADA networks," *Int. J. Crit. Infrastruct. Prot.*, vol. 42, no. June, p. 100612, 2023, doi: 10.1016/j.ijcip.2023.100612.

[13] K. Boeding, Matthew; Hempel, Michael; Sharif, Hamid; Jr, Juan Lopez; Perumalla, "A flexible OT testbed for evaluating on-device implementations of IEC-61850 GOOSE," *Int. J. Crit. Infrastruct. Prot.*, 2023.

[14] T. Aljohani and A. Almutairi, "A comprehensive survey of cyberattacks on EVs: Research domains, attacks, defensive mechanisms, and verification methods," *Def. Technol.*, vol. 42, 2024, doi: 10.1016/j.dt.2024.06.009.

[15] S. Pietro Ambrosio, Nicola d', Capodagli, Giulio, Perrone, Gaetano, Romano, "SCASS: Breaking into SCADA Systems Security," *Physica A*, 2024, doi: 10.1016/j.cose.2025.104315.

[16] L. M. Itzkin, Michael; Palmsten, Margaret L.; Buckley, Mark L.; Birchler, Justin J.; Torres-Gardia, "Developing a decision tree model to forecast runup and assess uncertainty in empirical formulations," *Coast. Eng.*, 2025.

[17] M. Bagriacik and F. E. B. Otero, "Multiple fairness criteria in decision tree learning," *Appl. Soft Comput.*, vol. 167, no. PA, p. 112313, 2024, doi: 10.1016/j.asoc.2024.112313.

[18] R. Widodo, Akdeas Oktanae; Setiawan, Bambang; Indraswari, "Machine Learning-Based Intrusion Detection on Multi-Class Imbalanced Dataset Using SMOTE," *Procedia Comput. Sci.*, vol. 234, pp. 578–583, 2024.

[19] M. G. Wijaya, M. F. Pinaringgi, A. Y. Zakiyyah, and Meiliana, "Comparative Analysis of Machine Learning Algorithms and Data Balancing Techniques for Credit Card Fraud Detection," *Procedia Comput. Sci.*, vol. 245, no. C, pp. 677–688, 2024, doi: 10.1016/j.procs.2024.10.294.

[20] A. A. Soomro *et al.*, "Data augmentation using SMOTE technique: Application for prediction of burst pressure of hydrocarbons pipeline using supervised machine learning models," *Results Eng.*, vol. 24, no. September, p. 103233, 2024, doi: 10.1016/j.rineng.2024.103233.

[21] E. Dazhi, J. Liu, M. Zhang, H. Jiang, and K. Mao, "RE-SMOTE: A Novel Imbalanced Sampling Method Based on SMOTE with Radius Estimation," *Comput. Mater. Contin.*, vol. 81, no. 3, pp. 3853–3880, 2024, doi: 10.32604/cmc.2024.057538.

[22] T. Ait tchakoucht, B. Elkari, Y. Chaibi, and T. Kousksou, "Random forest

with feature selection and K-fold cross validation for predicting the electrical and thermal efficiencies of air based photovoltaic-thermal systems," *Energy Reports*, vol. 12, no. July, pp. 988–999, 2024, doi: 10.1016/j.egyr.2024.07.002.

[23] 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.

[24] G. Phillips *et al.*, "Setting nutrient boundaries to protect aquatic communities: The importance of comparing observed and predicted classifications using measures derived from a confusion matrix," *Sci. Total Environ.*, vol. 912, no. July 2023, 2024, doi: 10.1016/j.scitotenv.2023.168872.

[25] 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.

[26] M. Mimura, "Impact of benign sample size on binary classification accuracy," *Expert Syst. Appl.*, vol. 211, no. June 2022, p. 118630, 2023, doi: 10.1016/j.eswa.2022.118630.

[27] 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.

[28] 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. April, p. 111169, 2022, doi: 10.1016/j.measurement.2022.111169.

[29] 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.