`

DISERTASI

SISTEM DETEKSI SERANGAN SIBER PADA JARINGAN SCADA PROTOKOL IEC 60870-5-104 MENGGUNAKAN PENDEKATAN MACHINE LEARNING

M. AGUS SYAMSUL ARIFIN

03013681924009

PROGRAM STUDI DOKTOR ILMU TEKNIK

BKU TEKNIK INFORMATIKA

FAKULTAS TEKNIK

UNIVERSITAS SRIWIJAYA

2023

HALAMAN PENGESAHAN

"SISTEM DETEKSI SERANGAN SIBER PADA JARINGAN SCADA PROTOKOL IEC 60870-5-104 MENGGUNAKAN MACHINE LEARNING"

DISERTASI

Diajukan untuk melengkapi salah satu syarat memperoleh gelar Doktor dalam bidang Ilmu Teknik Informatika

Oleh
M. AGUS SYAMSUL ARIFIN
NIM. 03013681924009

Palembang 31 Juli 2023

Promotor

Prof. Deris Stiawan, S.Kom., MT., Ph.D.
NIP. 197806172006041002

Ko-External Promotor

Associate Prof. Dr. Mohd Yazid Bin Idris

Mengetahui,

Dekan Fakultas Teknik

Prof. Dr. Eng. Ir. Joni Arliansyah, M.T.
NIP. 196706151995121002

Koordinator Prodi

Prof. Dr. Ir. Nukman, M.T.
NIP. 195903211987031001

HALAMAN PERSETUJUAN

Karya tulis ilmiah berupa laporan disertasi ini dengan judul "Sistem Deteksi Serangan Siber Pada Jaringan SCADA Protokol IEC 60870-5-104 Menggunakan pendekatan *Machine Learning*" telah dipertahankan dihadapan Tim Penguji Karya Tulis Ilmiah Program Studi Doktor Ilmu Teknik Fakultas Teknik Universitas Sriwijaya pada tanggal 31 Juli 2023

Palembang, 31 Juli 2023

Ketua
Dr. Bhakti Yudho Suprapto, ST., M.T.
NIP. 197502112003121002 ( )

Anggota

1. Dr. Didi Rosiyadi, S.Kom., M.Kom.
   NIP. 197504142005021002 ( )

2. Dr. Kurniabudi, S.Kom., M.Kom.
   NIDN. 1027067601 ( )

3. Dr. Yessi Novaria Kunang, ST., M.Kom.
   NIDN. 0226117501 ( )

Mengetahui,

Dekan Fakultas Teknik

Prof. Dr. Eng. Ir. Joni Arliansyah, M.T.
NIP. 196706151995121002

Koordinator Prodi

Prof. Dr. Ir. Nukman, M.T.
NIP. 195903211987031001

HALAMAN PERNYATAAN INTEGRITAS

Saya yang bertanda tangan di bawah ini:

Nama	: M. Agus Syamsul Arifin
NIM	: 03013681924009
Judul	: SISTEM DETEKSI SERANGAN SIBER PADA JARINGAN SCADA PROTOKOL IEC 60870-5-104 MENGGUNAKAN PENDEKATAN MACHINE LEARNING

Menyatakan bahwa ~~Laporan Akhir/Skripsi/Tesis~~/Disertasi* saya merupakan hasil karya sendiri didampingi ~~Tim pembimbing~~/Promotor dan Ko-promotor* dan bukan hasil penjiplakan/plagiat. Apabila ditemukan unsur penjiplakan/plagiat dalam ~~Laporan Akhir/Skripsi/Tesis~~/Disertasi* ini, maka saya bersedia menerima sanksi akademik dari Universitas Sriwijaya sesuai aturan yang berlaku.

Demikian pernyataan ini saya buat dalam keadaan sadar dan tanpa adanya paksaan dari siapapun.

Palembang, 31 Juli 2023

M. Agus Syamsul Arifin
NIM. 03013681924009

DAFTAR RIWAYAT HIDUP

M. Agus Syamsul Arifin dilahirkan di Kota Lubuklinggau pada tanggal 19 Agustus 1988. Anak pertama dari tiga bersaudara dari pasangan Alm. Samiyono dan Sudariyah. Pendidikan SD sampai dengan MA ditempuh di Kota kelahiran, Lubuklinggau. Setelah menyelesaikan pendidikan MA, melanjutkan ke jenjang Diploma Empat pada Program Studi Jaringan Radio dan Komputer Politeknik Negeri Semarang dan meraih gelar Sarjana Sains Terapan pada 2010.

Tahun 2012 mulai menjadi Guru TIK di salah satu SMK terkemuka di Kota Lubuklinggau, SMK Yadika Lubuklinggau. Dalam kurun waktu aktif mengajar, penulis memutuskan untuk melanjutkan studi S2 di bidang Teknik Informatika Universitas Bina Darma Palembang yang diselesaikan dalam kurun waktu 2 tahun, sehingga berhak memperoleh gelar Magister Komputer 2013.

Tahun 2014, penulis melanjutkan karier sebagai dosen di Universitas Bina Insan Lubuklinggau (dahulu STMIK Musirawas dan berkembang menjadi universitas pada tahun 2019). Selama menjadi dosen, penulis aktif dalam hibah, salah satunya hibah Penelitian Dosen Pemula (PDP) pada tahun 2018. Selain menjadi dosen tetap yayasan, penilis dipercaya untuk mengemban tugas tambahan sebagai Sekertaris Program Studi Teknik Informatika (2016-2017) dan Kepala Information and Communication Technology (2017-2019).

Tahun 2019, penulis memutuskan untuk melanjutkan pendidikan S3 pada Program Studi Doktor Ilmu Teknik Universitas Sriwijaya dengan bidang kajian Teknik Informatika dengan Skema pembiayaan beasiswa BPPDN tahun 2019. Bidang penelitian disertasi penulis fokus pada deteksi serangan siber pada jaringan SCADA menggunakan pendekatan *machine learning*. Dalam melaksanakan penelitian disertasi, penulis dibimbing dan diarahkan oleh Associate Prof. Deris Stiawan, S.Kom.,MT.,Ph.D selaku promotor dan Associate Prof. Dr. Mohd Yazid Bin Idris sebagai ko-promotor.

KATA PENGANTAR

Puji syukur kita panjatkan kehadirat Allah SWT, dimana berkat rahmat dan karunia-Nya disertasi ini dapat diselesaikan. Disertasi ini diberi judul "SISTEM DETEKSI SERANGAN SIBER PADA JARINGAN SCADA PROTOKOL IEC 60870-5-104 MENGGUNAKAN PENDEKATAN MACHINE LEARNING". Usulan disertasi ini merupakan salah satu persyaratan dalam menyelesaikan studi pada Program Doktor Ilmu Teknik Universitas Sriwijaya.

Shalawat serta salam kita panjatkan kepada junjungan besar Nabi Muhammad SAW yang selalu memberikan syafaat dalam perjalanan kita. Meskipun penulis telah berupaya untuk menyajikan disertasi yang terbaik, namun masih terdapat kekurangan, oleh karenanya kritik serta saran yang membangun sangat diperlukan untuk kesempurnaan disertasi ini.

Selesainya disertasi ini tentunya tidak terlepas dari dukungan banyak pihak, oleh karenanya pada kesempatan ini penulis ingin mengucapkan terima-kasih kepada :

1. Keluarga tercinta Almarhum Bapak dan Ibu, orang tua saya yang selalu memberikan ridho dan do'a restu untuk setiap perjalan dan perjuangan saya selama menempuh pendidikan. Istri dan anak-anakku, atas pengertian dan pengorbanannya, serta adik - adikku yang selalu mendukung.
2. Prof. Deris Stiawan, S.Kom., MT., Ph.D selaku Promotor yang dengan sabar memberikan banyak sekali dukungan dan pengorbanan yang tidak dapat disebutkan satu persatu.

3. Bapak Assoc. Prof. Dr. Moh. Yazid Idris selaku ko-promotor yang telah memberikan dukungan dalam penelitian disertasi ini.
4. Dosen-dosen program Doktor Ilmu Teknik, atas ilmu dan kesabarannya.
5. Teman – teman seperjuangan di Research for Life yang telah memberikan dukungannya baik moril maupun materil.
6. Teman – teman sejawat Fakultas Ilmu Komputer Universitas Bina Insan Lubuklinggau, khususnya Program Studi Rekayasa Sistem Komputer yang telah memberikan semangat.
7. Adik-adik dan rekan-rekan di COMNETS RG UNSRI, yang telah bersedia berbagi pengalaman dan ilmunya, Rekan-rekan seperjuangan Program Studi Doktor Ilmu Teknik yang selalu memberikan inspirasi dan motivasi baik secara langsung maupun tidak langsung.
8. Yayasan Dwi Tunggal Palembang, Rektor Universitas Bina Insan dan Ketua STMIK Musi Rawas yang telah memberikan Izin untuk melanjutkan Pendidikan Doktor di Universitas Sriwijaya.

Terimakasih atas dukungan yang diberikan baik secara moril dan materil, semoga kebaikannya mendapatkan pahala yang setimpal dari Allah SWT. Akhir kata, semoga disertasi ini telah memenuhi persyaratan dan dapat diterima sebagai laporan hasil penelitian saya selama menempuh pendidikan Doktoral di Universitas Sriwijaya.

Penulis

M. Agus Syamsul Arifin

SUMMARY

CYBER ATTACK DETECTION SYSTEM ON SCADA NETWORK IEC 60870-5-104 PROTOCOL USING MACHINE LEARNING APPROACH
Doctoral Research,

M. Agus Syamsul Arifin; Supervised by Prof. Deris Stiawan, S. Kom., MT., Ph. D and Dr. Mohd Yazid Idris

xvi + 135 Page, 24 table, 67 pictures, 6 attachement

Supervisory and Data Acquisition (SCADA) plays an important role in industry by providing process automation, centralized control and monitoring processes. SCADA is designed for closed areas with special protocols that are isolated from the internet, but modern SCADA systems are required to be connected to one or more other network protocols to make it easier to access the SCADA system from heterogeneous networks, thus increasing vulnerability in this system. This phenomenon is interesting to study because there are still few researchers conducting a comprehensive discussion of security on the SCADA network, besides the performance of open source IDS (Intrusion Detection System) such as Snort and Suricata is less efficient in detecting disturbances on the SCADA network so that this research has the aim of designing an ideal IDS for SCADA networks using a machine learning approach. To produce an IDS that is able to work well to detect attacks in the SCADA network, a relevant dataset is needed, then the attack patterns recognition is carried out to obtain relevant features that will be used as training data for the IDS model, the selection of machine learning algorithms that are relevant to the SCADA network by paying attention to the performance of the resulting IDS model. This research has the novelty of finding attack patterns on the IEC 60870-5-104 protocol. The datasets used are the dataset from maynard_2018 and the comnets_scada_iec104 dataset. The comnets_scada_iec104 dataset was created using a physical testbed close to the actual conditions of the SCADA system. The highest accuracy of the IDS model when using the maynard_2018 dataset is 98.84% with the decision tree algorithm. The highest accuracy of the IDS model using the comnets_scada_iec104 dataset was obtained using the decision tree and random forest algorithms with the same accuracy level of 99.05%. This accuracy was obtained by adding a random under-sampling method.

Keyword **:** IDS SCADA, IEC-60870-5-104, *machine learning, Random Under sampling, Random Over sampling, SMOTE*
Refrence : 123 (2009 – 2023)

RINGKASAN

SISTEM DETEKSI SERANGAN SIBER PADA JARINGAN SCADA PROTOKOL IEC 60870-5-104 MENGGUNAKAN MACHINE LEARNING
Disertasi,

M. Agus Syamsul Arifin; Dipromotori oleh Prof. Deris Stiawan, S. Kom., MT., Ph. D dan Dr. Mohd Yazid Idris

xvi + 135 Halaman, 24 tabel, 67 bagan, 6 Lampiran

Saat ini Supervisory and Data Acquisition (SCADA) memegang peranan penting di industri dengan menyediakan proses otomisasi, pengendalian terpusat dan proses monitoring. SCADA di desain untuk area tertutup dengan protokol khusus yang terisolasi dari internet, namun sistem SCADA modern diharuskan terhubung dengan satu atau lebih protokol jaringan lain untuk mempermudah dalam mengakses sistem SCADA dari jaringan Heterogenous sehingga meningkatkan kerentanan dalam sistem ini. Fenomena ini menarik untuk di kaji karena masih sedikit peneliti melakukan pembahasan yang komprehensif terhadap keamanan pada jaringan SCADA, selain itu performa IDS (Intrusion Detection System) open source sperti Snort dan Suricata kurang efisien dalam mendeteksi gangguan pada jaringan SCADA sehingga penelitian ini memiliki tujuan untuk merancang IDS yang ideal untuk jaringan SCADA dengan menggunakan pendekatan machine learning. Untuk menghasilkan IDS yang mampu bekerja baik mendeteksi serangan dalam jaringan SCADA dibutuhkan dataset yang relevan, kemudian pengenalan pola serangan dilakukan untuk mendapatkan fitur relevan yang akan digunakan sebagai data latih untuk model IDS, selanjutnya pemilihan algoritma machine leraning yang relevan untuk jaringan SCADA dengan memperhatikan performa dari model IDS yang dihasilkan. Penelitian ini memiliki kebaharuan yaitu menemukan pola serangan pada protokol IEC 60870-5-104. Dataset yang digunakan adalah dataset dari maynard_2018 dan dataset comnets_scada_iec104. Dataset comnets_scada_iec104 dibuat menggunakan testbed fisik dengan memperhatikan kondisi nyata sistem SCADA. Akurasi tertinggi pada dari model IDS ketika menggunakan dataset maynard_2018 adalah sebesar 98,84% dengan algoritma decision tree. Akurasi tertinggi pada model IDS menggunakan dataset comnets_scada_iec104 didapatkan menggunakan algoritma decision tree dan random forest dengan tingkat akurasi yang sama sebesar 99,05% akurasi ini didapat dengan menambahkan metode random under-sampling.

Kata Kunci : IDS SCADA, IEC-60870-5-104, *machine learning, Random Under sampling, Random Over sampling, SMOTE*
Kepustakaan : 123 (2009 – 2023)

DAFTAR ISI

Halaman

DAFTAR GAMBAR

DAFTAR TABEL

`

BAB I

PENDAHULUAN

Industrial Control System (ICS) dalam khususnya *Supervisory and Data Acquisition* (SCADA) memegang peranan penting dalam industri *modern* dengan menyediakan proses otomisasi, pengendalian terpusat dan proses monitoring (Asghar et al., 2019), SCADA di desain untuk area tertutup dengan protokol khusus yang terisolasi dari internet menggunakan *firewall* (Gao et al., 2010), (Yadav & Paul, 2021), (Sverko et al., 2022), namun sistem SCADA *modern* diharuskan terhubung dengan satu atau lebih protokol jaringan lain (Mai et al., 2019) untuk mempermudah dalam mengakses sistem SCADA dari jaringan Heterogenous. Interkoneksi SCADA ke protokol jaringan lainnya seperti TCP/IP meningkatkan kerentanan sistem SCADA dalam menerima gangguan/serangan *cyber* dari luar (Volkova et al., 2019), (X. Wang & Foo, 2018).

Akibat semakin meningkatnya kerentanan sistem SCADA membuat deteksi serangan dalam sistem SCADA menjadi tantangan pada penelitian dalam bidang keamamnan *Cyber* untuk membangun sebuah sistem IDS yang *robust*. Salah satu metode yang digunakan untuk membangun IDS (*Intrusion Detection System*) pada jaringan SCADA adalah menggunakan metode *machine learning* namun dalam membangun IDS menggunakan *machine learning* dibutuhkan dataset yang *proper* untuk dapat menghasilkan IDS yang dapat mendeteksi serangan dalam jaringan SCADA, dengan memperhatikan dataset yang akan digunakan akan meningkatkan kehandalan IDS tersebut dalam hal ini akurasi yang baik dan alarm palsu yang

rendah. Menurut (X. Wang & Foo, 2018) dalam membuat dataset yang baik pada IDS SCADA adalah dengan memperhatikan proses *input, controller,* dan *Network* dalam hal ini *traffic* data normal dan *traffic* data yang serangan sehingga dalam pembuatan dataset dalam penelitian ini menggunakan *testbed* fisik dengan scenario serangan yang beragam seperti *port scan, brute force, icmp flood, syn flood, xmas* dan IEC104 *flood* dataset dari penelitian ini sudah di publish pada Zenodo.

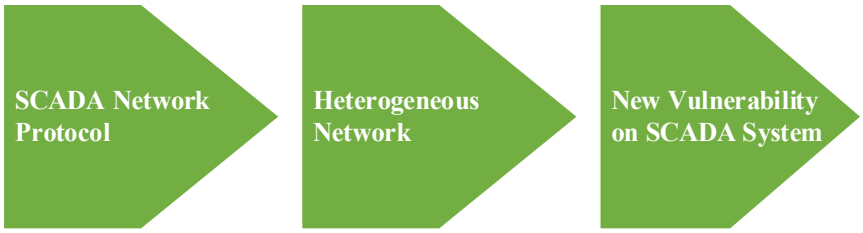
1.1 Latar Belakang

Serangan pada *Industrial Control System* (ICS) termasuk sistem *Supervisory Control and Data Acquisiton* (SCADA) semakin meningkat dengan skala dan teknik yang semakin beragam (Bhamare et al., 2019), trend ini yang menyebabkan sistem komputer yang digunakan pada SCADA rentan terhadap serangan *cyber* maupun *malware* (Linda et al., 2009), fenomena ini menarik untuk di kaji karena masih sedikit peneliti melakukan pembahasan yang komprehensif terhadap keamanan pada jaringan SCADA (Rubio et al., 2019), (Ayodeji et al., 2020). Semakin terbukanya sistem SCADA ke protokol jaringan lain yang bertujuan untuk menurunkan *cost,* standarisasi perangkat keras, dan perangkat lunak (Rubio et al., 2019) yang sebelumnya tertutup ke protokol jaringan terbuka (heterogen) (Pliatsios et al., 2020) dan berbagai protkokol SCADA lainnya seperti IEC, OPC UA, DNP3 (Shosha et al., 2011) dan Modbus ataupun protokol TCP/IP (Ullah & Mahmoud, 2018) dapat meningkatkan jumlah celah keamanan pada jaringan penghubung perangkat industri (Waagsnes & Ulltveit-Moe, 2018). Hasil penelitian yang dilakukan (Dakheel et al., 2019) salah satu masalah keamanan dalam sistem SCADA adalah rendahnya *compute resource* pada sistem SCADA itu sendiri,

sehingga tidak memungkinkan untuk menerapkan sistem keamanan standar seperti pada sistem jaringan tradisional, selain itu sistem SCADA pada awal pengembangan dirancang hanya untuk keamanan fisik dan hampir tidak ada perhatian dalam keamanan *cyber*.

Beberapa penelitian juga menemukan celah keamanan pada Protokol Sistem SCADA yang mengakibatkan penyerang dapat melakukan berbagai skenario serangan pada sistem jaringan SCADA seperti dijelaskan pada penelitian (Darwish et al., 2016) yang menemukan celah keamanan pada protokol DNP3 dengan cara melakukan simulasi serangan MiTM, kemudian pada penelitian (Radoglou-Grammatikis et al., 2019) melakukan pengujian serangan pada protokol IEC-60870-5-104 dan mengukur bobot ancaman pada setiap serangan yang dilakukan, hal ini menunjukkan protokol SCADA yang digunakan dan terkoneksi ke jaringan Heterogenous rentan terhadap serangan yang mengarah ke perangkat infrastruktur jaringan yang menggunakan sistem SCADA sebagai protokol komunikasinya, kerentanan ini dapat dimanfaatkan penyerang untuk melakukan *malisious activity* pada perangkat industri. Kerentanan lain pada sistem SCADA yang terkoneksi ke jaringan Heterogen yang dijelaskan pada peneltitian yang dilakukan (Samtani et al., 2018) dengan menggunakan teknik *text mining* pada mesin pencari SHODAN, dimana mesin pencari ini dapat mendeteksi perangkat – perangkat SCADA maupun IoT yang terhubung ke internet ini menunjukkan jika sistem SCADA sangat rentan apabila SCADA terkoneksi ke jaringan Heterogen, dalam peneltiannya yang lain (Samtani et al., 2016) juga mengkategorikan tingkat kerentanan pada perangkat SCADA yang terdeteksi pada SHODAN. Menurut (Irmak & Erkek, 2018)

penerapan *port default* untuk komunikasi perangkat dalam industri yang menggunakan protokol SCADA memudahkan penyerang untuk mengeksploitasi perangkat – perangkat industri tersebut. Gambar 1.1 berikut merupakan ilustrasi yang penulis buat berdasarkan pengamatan penulis pada penelitian yang menyatakan semakin terbuka komunikasi SCADA ke jaringan Heterogeneous akan menimbulkan kerentanan baru dalam jaringan SCADA.



Gambar 1.1 Ilustrasi akibat terkoneksinya sistem SCADA ke jaringan terbuka.

Pada penelitian ini akan berfokus pada protokol IEC-60870-5-104 (IEC 104) karena protokol ini banyak digunakan pada industri (Mai et al., 2019), (Carlini et al., 2019), seperti industri pembangkit tenaga listrik khususnya di Indonesia yang digunakan Perusahaan Listrik Negara (PLN). Kerentanan akibat interkoneksi SCADA juga menjadi masalah pada PLN dimana RTU yang ditempatkan dilapangan memiliki system keamanan dari serangan siber yang terbatas. Salah satu alasan banyaknya penggunaan protokol IEC 104 dalam industri listrik adalah karena protokol IEC 104 mendukung *Automation Generation Control* (AGC) yang merupakan sebuah algoritma yang dapat mengatur keseimbangan energi listrik dalam area geografis yang besar (Mai et al., 2019).

Secara umum paket data dari protokol SCADA akan di enkapskulasi ke protokol TCP (*Transmission Control Protocol*) sebelum data dikirimkan (Eden et al., 2015), (Hou et al., 2016) sehingga teknik serangan yang dilakukan pada sistem jaringan tradisional dapat dilakukan pada sistem SCADA yang menggunakan protokol IEC 104 begitu juga cara mengatasinya, teknik IDS (*Intrusion Detection System*) pada sistem jaringan tradisional dapat diterapkan pada sistem SCADA dengan penyesuaian agar dapat diterapkan. Penelitian ini akan menggunakan dataset yang dibuat oleh (Maynard et al., 2018) dan dataset yagn dihasilkan dari penelitian ini dalam bentuk raw data dengan *file* brekstensi pcap. Pada dataset (Maynard et al., 2018) berisi serangan MiTM (*Man in the Middle)* yang menyerang salah satu RTU dengan mengubah *Cause of Transmission (CoT)* RTU tersebut, dataset ini juga di pakai pada penelitian (Waagsnes & Ulltveit-Moe, 2018) dan (Grammatikis et al., 2020). Penelitian (Waagsnes & Ulltveit-Moe, 2018) menggunakan IDS dengan *signature base* untuk mendeksi serangan pada SCADA mendapatkan *latency* yang tinggi dalam mendeteksi aktifitas berbahaya pada jaringan SCADA, kemudian pada penelitian IDS yang dilakukan (Grammatikis et al., 2020) untuk mendeteksi anomali pada jaringan SCADA dengan protokol IEC 104 mendapatkan F1 score 87% dengan akurasi mencapai 98%. Dalam perkembangannya banyak penelitian pada IDS SCADA masih menggunakan dataset jaringan komputer konvensional yang menurut (Rodofile et al., 2017) dataset yang berasal dari KDDcup99 sudah tidak relevan untuk digunakan pada IDS SCADA. Pada dataset comnets_scada_iec104 ini terdapat aktifitas port scan, brute

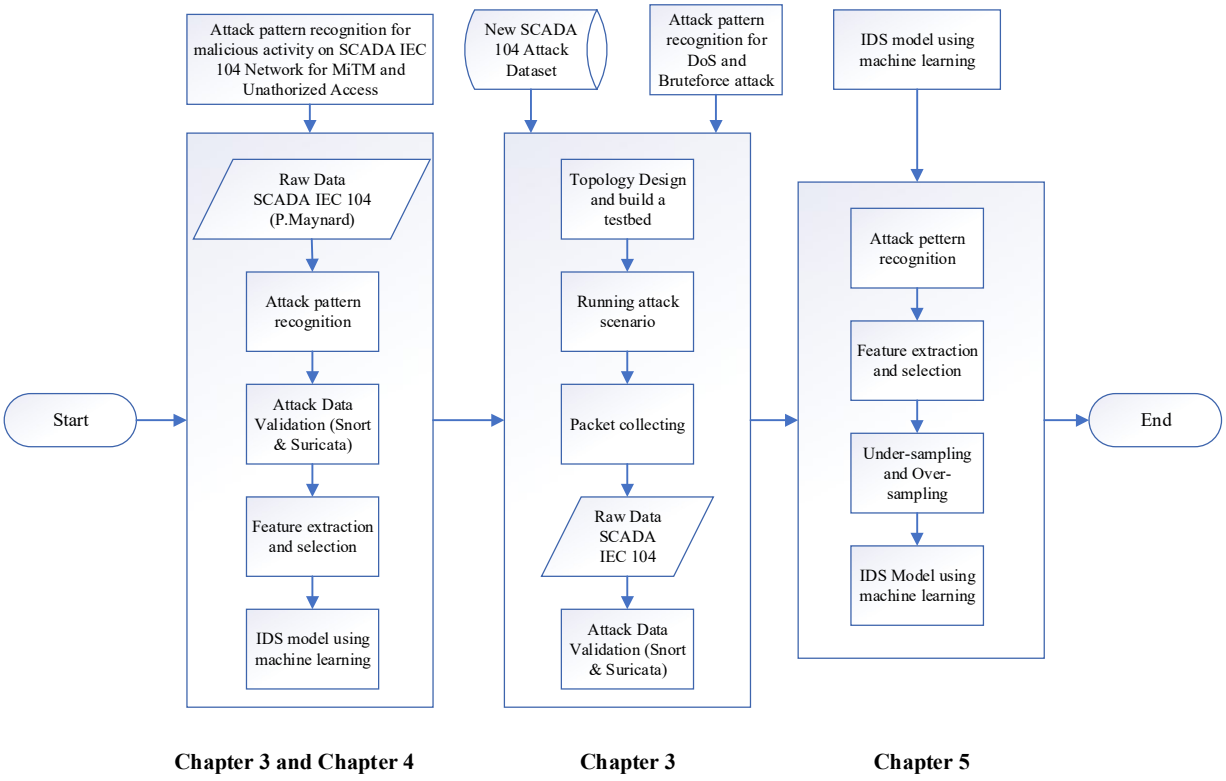
force dan serangan DoS. Serangan DoS yang ada pada dataset yaitu ICMP *flood* (ping *flood*), Syn *flood*, Xmas dan IEC 104 *flood*.

Menurut (Texas, 2012) tantangan dalam membangun IDS yang khusus dibangun untuk jaringan SCADA adalah (i) *aviability* dan *timeliness* sangat penting sehingga istilah CIA (*confidentiality-integrity-availability*) dalam mendesain keamanan dalam dunia *cyber* menjadi AIC (*availability-integrity-confidentiality*) untuk sistem SCADA, (ii) Tantangan memori atau *compute resource* yang terbatas pada perangkat lapangan SCADA, dan (iii) adanya keterhubungan antara jaringan *cyber-physical* dalam sistem SCADA dan yang mendasari sumber listrik yang membuat serangan dalam jaringan SCADA memiliki efek berjenjang yang mampu menyerang sistem fisik yang menjadi dasar SCADA. Untuk membangun sebuah IDS berbasis pembelajaran mesin dibutuhkan dataset yang relevan dengan system jaringan SCADA, dataset ini harus merangkum semua data baik normal dari jaringan SCADA dan serangan.

Dari uraian latar belakang dan analisis dari penulis maka diperlukan sebuah model IDS yang *robust* pada sistem jaringan SCADA untuk mengatasi kerentanan akibat terbukanya koneksi pada sistem SCADA ke jaringan Heterogen, IDS tersebut harus memiliki *false alarm* yang rendah dan akurasi deteksi yang tinggi untuk menghasilkan IDS yang *robust* tersebut di butuhkan dataset yang baik dengan variasi data normal dan data serangan yang beragam untuk mendukung sistem pembelajaran pada IDS berbasis *machine learning* dan menurut (X. Wang & Foo, 2018) dalam membuat dataset yang baik pada IDS SCADA adalah dengan

memperhatikan proses *input, controller,* dan *Network* dalam hal ini *traffic* data normal dan *traffic* data yang serangan.

Gambar 1.2 berikut menunjukkan alur kerja yang dilakukan dan kontribusi dari penelitian ini.



Gambar 1.2 Alur kerja dan kontribusi penelitian

Kontribusi dari penelitian ini adalah pengenalan pola serangan yang relevan pada jaringan SCADA IEC 104 dan dataset yang relevan untuk membangun sebuah model IDS menggunakan machine learning karena diambil dari *testbed* yang relevan. Kontribusi pada masyarakat adalah jika model ini diterapkan akan menjadi sebuah system pertahanan pertama dalam menghadapi serangan siber pada jaringan SCADA. Kebaharuan dari penelitian ini adalah menemukan pola serangan pada jaringan SCADA pada protocol IEC 104.

1.2 Perumusan Masalah

Isu pada keamanan SCADA adalah Interkoneksi SCADA ke jaringan Heterogen yang tidak dapat dihindari disebabkan kebutuhan dari industri dalam menghemat *cost* dan metode deteksi yang belum efisien khusus pada sistem SCADA kemudian standarisasi perangkat keras dan lunak yang menyebabkan terbukanya kerentanan baru pada sistem SCADA. Dari studi literatur penelitian yang sudah penulis lakukan masih terdapat peluang untuk penelitian deteksi serangan dalam jaringan SCADA diantaranya, (i) masih sedikitnya penelitian yang membahas deteksi serangan pada sistem scada menggunakan metode *machine learning* khususnya pada protokol IEC-60870-5-104, (ii) sedikitnya penelitian yang membahas dataset yang relevan untuk IDS dalam jaringan SCADA, (iii) Penelitian yang sudah dilakukan belum menjawab masalah yang ada dalam IDS SCADA khususnya penelitian yang memaparkan hasil pengujian dan perbandingan performa IDS pada sistem SCADA pada protokol IEC-60870-5-104 menggunakan *machine learning*, (iv) masih sedikit penelitian yang membahas pola serangan pada jaringan sistem SCADA IEC 60870-5-104. Berdasarkan peluang tersebut maka penulis akan membuat sebuah *testbed* sistem SCADA IEC 60870-5-104 kemudian membuat dataset serangan dan membangun model IDS yang sesuai untuk protokol SCADA IEC 60870-5-104. Penulis menggunakan dataset (Maynard et al., 2018) dan dataset yang penulis bangun. Dengan menggunakan dua dataset yang berbeda akan memberikan data yang baik dalam mengenali pola serangan di jaringan SCADA IEC 104. Dalam penelitian ini akan membahas solusi dari isu yang menjadi landasan penelitian ini :

1. Bagaimana membuat dataset IDS jaringan SCADA yang relevan berdasarkan pola paket data dalam jaringan SCADA khususnya protokol IEC 104 karena kurangnya dataset yang relevan untuk IDS SCADA protokol IEC 104 ?
2. Bagaimana membangun model IDS pada untuk SCADA dengan tingkat akurasi yang tinggi dengan menggunakan *machine learning* ?
3. Bagaimana mengukur performa IDS pada jaringan SCADA dalam mendeteksi gangguan/serangan dalam jaringan SCADA ?

1.3 Tujuan Penelitian

Tujuan umum dari penelitian ini adalah untuk mendeteksi gangguan/ *malicious activity* dalam jaringan SCADA dengan performa yang baik, kemudian secara khusus tujuan dari penelitian ini adalah :

1. Menghasilkan dataset serangan relevan berdasarkan data lalulintas pada jaringan SCADA IEC 104 dan memiliki jenis serangan yang bervariasi.
2. Menemukan pola serangan yang dapat terjadi pada jaringan SCADA.
3. Merancang model IDS pada SCADA IEC 60870-5-104 dalam mendeteksi gangguan/serangan pada jaringan SCADA menggunakan *machine learning*.
4. Menguji Performa model IDS pada jaringan SCADA IEC 60870-5-104.

1.4 Ruang Lingkup Penelitian

Berdasarkan latar belakang, perumusan masalah dan tujuan penelitian, maka ruang lingkup dari penelitian ini agar adalah :

1. Penelitian ini berfokus dalam pengenalan pola serangan dan data ekstraksi fitur dalam jaringan SCADA pada protokol IEC-60870-5-104

2. Pengujian dilakukan pada protokol SCADA dengan menggunakan dataset yang berupa RAW data dengan ekstensi pcap dari *payloads* data yang dihasilkan pada *testbed* penelitian (Maynard et al., 2018) dan dengan RAW data dari *testbed* SCADA IEC 60870-5-104 penelitian ini.
3. Pengujian pada penelitian ini dilakukan untuk mendeteksi *port scan*, TESTFR (*Test Frame*), STARTDT (*Start Data Transfer*) yang merupakan *unauthorise access* dan paket yang dirubah oleh serangan MiTM yaitu *Cause of Transmission (CoT)* yang memiliki nilai 42 (*Unknown)* untuk dataset yang dihasilkan oleh P.Maynard (Maynard et al., 2018) dan serangan *port scan, brute force,* ICMP *flood*, Syn *flood*, Xmas dan IEC 104 *flood* pada comnets_scada_iec104 ini.
4. Tidak membahas sistem pencegahan serangan IPS (*Intrusion Preventive System*).

1.5 Sistematika Penulisan

Agar memperoleh gambaran jelas mengenai penelitian ini, maka dibuatlah suatu sistematika penulisan yang berisi gambaran dalam tiap bab penelitian ini, yaitu:

1. **BAB I Pendahuluan**
   Bab ini menjelaskan tentang latar belakang masalah, perumusan masalah, tujuan penelitian, dan ruang lingkup penelitian.
2. **BAB II Landasan Teori**
   Bab ini menjelaskan mengenai *literature review* yang berhubungan dengan masalah dalam penelitian SCADA yang penulis lakukan saat ini.

3. **BAB III Metodologi Penelitian**

   Bab ini menjelaskan tahapan untuk menyelesaikan penelitian dan proses yang dilakukan selama penelitian. Pengenalan pola serangan, ekstraksi data, dan seleksi fitur pada dataset (Maynard et al., 2018) dan dataset yang dihasilkan menggunakan *testbed* pada penelitian ini juga dijelaskan pada bab ini.

4. **BAB IV Hasil dan Pembahasan Deteksi *Malicious Activity* pada sistem SCADA IEC 60870-5-104**

   Bab ini menjelaskan Hasil dari pengujian dan pengukuran model IDS menggunakan dataset (Maynard et al., 2018) dan dataset comnets_scada_iec104 yang dihasilkan menggunakan *testbed* pada penelitian ini.

5. **BAB V Hasil dan Pembahasan Metode Undersampling dan Oversampling pada IDS SCADA IEC 60870-5-104**

   Bab ini menjelaskan metode untuk mengatasi data yang imbalance pada dataset dengan teknik Undersampling dan Oversampling dan membandingkan performanya. Dataset comnets_scada_iec_104 yang digunakan pada bab ini adalah dataset yang penulis buat menggunakan *testbed* pada penelitian ini.

6. **BAB VI Kesimpulan**

   Bab ini menjelaskan kesimpulan dari hasil penelitian yang penulis lakukan.

DAFTAR PUSTAKA

Aamir, M., & Zaidi, S. M. A. (2019). DDoS attack detection with feature engineering and machine learning: the framework and performance evaluation. *International Journal of Information Security*, *18*(6), 761–785. https://doi.org/10.1007/s10207-019-00434-1

Abbas, S. G., Hashmat, F., Shah, G. A., & Zafar, K. (2021). Generic signature development for IoT Botnet families. *Forensic Science International: Digital Investigation*, *38*, 301224. https://doi.org/10.1016/j.fsidi.2021.301224

Al-Asiri, M., & El-Alfy, E. S. M. (2020). On Using Physical Based Intrusion Detection in SCADA Systems. *Procedia Computer Science*, *170*(2019), 34–42. https://doi.org/10.1016/j.procs.2020.03.007

Al, S., & Dener, M. (2021). STL-HDL: A new hybrid network intrusion detection system for imbalanced dataset on big data environment. *Computers and Security*, *110*, 102435. https://doi.org/10.1016/j.cose.2021.102435

Alhaidari, F. A., & Al-Dahasi, E. M. (2019). New approach to determine DDoS attack patterns on SCADA system using machine learning. *2019 International Conference on Computer and Information Sciences, ICCIS 2019*, 1–6. https://doi.org/10.1109/ICCISci.2019.8716432

Alkasassbeh, M. (2017). an Empirical Evaluation for the Intrusion Detection Features Based on Machine Learning and Feature Selection Methods. *ArXiv*.

Almaiah, M. A., Almomani, O., Alsaaidah, A., Al-Otaibi, S., Bani-Hani, N., Hwaitat, A. K. Al, Al-Zahrani, A., Lutfi, A., Awad, A. B., & Aldhyani, T. H. H. (2022). Performance Investigation of Principal Component Analysis for Intrusion Detection System Using Different Support Vector Machine Kernels. *Electronics*, *11*(21), 3571. https://doi.org/10.3390/electronics11213571

Almalawi, A., Fahad, A., Tari, Z., Khan, A. I., Alzahrani, N., Bakhsh, S. T., Alassafi, M. O., Alshdadi, A., & Qaiyum, S. (2020). Add-on anomaly threshold technique for improving unsupervised intrusion detection on SCADA data. *Electronics (Switzerland)*, *9*(6), 1–20. https://doi.org/10.3390/electronics9061017

Amoah, R., Camtepe, S., & Foo, E. (2016). Formal modelling and analysis of DNP3 secure authentication. *Journal of Network and Computer Applications*, *59*, 345–360. https://doi.org/10.1016/j.jnca.2015.05.015

Ananin, E. V., Nikishova, A. V., & Kozhevnikova, I. S. (2017). Port scanning detection based on anomalies. *11th International IEEE Scientific and Technical Conference &Amp;Quot;Dynamics of Systems, Mechanisms and Machines&Amp;Quot;, Dynamics 2017 - Proceedings*, *2017-Novem*, 1–5. https://doi.org/10.1109/Dynamics.2017.8239427

Arifin, M. A. S., Stiawan, D., Idris, M. Y., & Budiarto, R. (2021). The trends of supervisory control and data acquisition security challenges in heterogeneous networks. *Indonesian Journal of Electrical Engineering and Computer Science*, *22*(2), 266–275. https://doi.org/10.11591/ijeecs.v22.i2.pp266-275

Arifin, M. A. S., Stiawan, D., Susanto, Prasetya, D., Yazid Idris, M., & Budiarto, R. (2021). Malicious Activity Recognition on SCADA Network IEC 60870-

5-104 Protocol. *2021 International Conference on Technology and Policy in Energy and Electric Power (ICT-PEP)*, *3*(September), 46–51. https://doi.org/10.1109/ict-pep53949.2021.9601066

Arifin, M. A. S., Stiawan, D., Susanto, Rejito, J., Idris, M. Y., & Budiarto, R. (2021). Denial of Service Attacks Detection on SCADA Network IEC 60870-5-104 using Machine Learning. *International Conference on Electrical Engineering, Computer Science and Informatics (EECSI) 2021*, *8*(October), 228–232. https://doi.org/10.23919/eecsi53397.2021.9624255

Artur, M. (2021). Review the performance of the Bernoulli Naïve Bayes Classifier in Intrusion Detection Systems using Recursive Feature Elimination with Cross-validated selection of the best number of features. *Procedia Computer Science*, *190*(2019), 564–570. https://doi.org/10.1016/j.procs.2021.06.066

Asghar, M. R., Hu, Q., & Zeadally, S. (2019). Cybersecurity in industrial control systems: Issues, technologies, and challenges. *Computer Networks*, *165*. https://doi.org/10.1016/j.comnet.2019.106946

Ayodeji, A., Liu, Y. kuo, Chao, N., & Yang, L. qun. (2020). A new perspective towards the development of robust data-driven intrusion detection for industrial control systems. *Nuclear Engineering and Technology*, *52*(12), 2687–2698. https://doi.org/10.1016/j.net.2020.05.012

Bagui, S., & Li, K. (2021). Resampling imbalanced data for network intrusion detection datasets. *Journal of Big Data*, *8*(1). https://doi.org/10.1186/s40537-020-00390-x

Bhamare, D., Zolanvari, M., Erbad, A., Jain, R., Khan, K., & Meskin, N. (2019). Cybersecurity for industrial control systems: A survey. *Computers & Security*, *89*, 101677. https://doi.org/https://doi.org/10.1016/j.cose.2019.101677

Bhattacharyya, D. K., & Kalita, J. K. (2013). Network anomaly detection: A machine learning perspective. *Network Anomaly Detection: A Machine Learning Perspective*, 1–337.

Biau, G., & Rouvière, B. C. L. (2019). Accelerated gradient boosting. *Machine Learning*, *108*(6), 971–992. https://doi.org/10.1007/s10994-019-05787-1

Buczak, A. L., & Guven, E. (2016). A Survey of Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection. *IEEE Communications Surveys and Tutorials*, *18*(2), 1153–1176. https://doi.org/10.1109/COMST.2015.2494502

Carlini, E. M., Neri, S., Zaretti, L., Coppoli, E., Campisano, L., Lattuada, G., Fazion, M., Ferretti, P., & Manocchio, P. (2019). A new approach for sending dispatching orders using protocol IEC 60870-5-104. *2019 AEIT International Annual Conference, AEIT 2019*, 1–4. https://doi.org/10.23919/AEIT.2019.8893376

Chandrashekar, G., & Sahin, F. (2014). A survey on feature selection methods. *Computers and Electrical Engineering*, *40*(1), 16–28. https://doi.org/10.1016/j.compeleceng.2013.11.024

Dakheel, A. H., Ucan, O. N., Bayat, O., & Jasim, H. H. (2019). *CYBER ATTACK DETECTION IN REMOTE TERMINAL UNIT OF SCADA SYSTEMS*. *8*(3), 193–203.

Darwish, I., Igbe, O., & Saadawi, T. (2016). Vulnerability assessment and

experimentation of smart grid DNP3. *Journal of Cyber Security and Mobility*, *5*(1), 23–54. https://doi.org/10.13052/jcsm2245-1439.513

Davis, J. J., & Clark, A. J. (2011). Data preprocessing for anomaly based network intrusion detection: A review. *Computers and Security*, *30*(6–7), 353–375. https://doi.org/10.1016/j.cose.2011.05.008

de Toledo, T., & Torrisi, N. (2019). Encrypted DNP3 Traffic Classification Using Supervised Machine Learning Algorithms. *Machine Learning and Knowledge Extraction*, *1*(1), 384–399. https://doi.org/10.3390/make1010022

Dhote, Y., Agrawal, S., & Deen, A. J. (2016). A Survey on Feature Selection Techniques for Internet Traffic Classification. *Proceedings - 2015 International Conference on Computational Intelligence and Communication Networks, CICN 2015*, 1375–1380. https://doi.org/10.1109/CICN.2015.267

Divekar, A., Parekh, M., Savla, V., Mishra, R., & Shirole, M. (2018). Benchmarking datasets for Anomaly-based Network Intrusion Detection: KDD CUP 99 alternatives. *Proceedings on 2018 IEEE 3rd International Conference on Computing, Communication and Security, ICCCS 2018*, 1–8. https://doi.org/10.1109/CCCS.2018.8586840

Dua, S., & Du, X. (2011). Data Mining and Machine Learning in Cybersecurity. *Data Mining and Machine Learning in Cybersecurity*. https://doi.org/10.1201/b10867

Eden, P., Blyth, A., Burnap, P., Cherdantseva, Y., Jones, K., & Soulsby, H. (2015). *A Forensic Taxonomy of SCADA Systems and Approach to Incident Response*. 42–51. https://doi.org/10.14236/ewic/ics2015.5

Egger, M., Eibl, G., & Engel, D. (2020). Comparison of Approaches for Intrusion Detection in Substations using the IEC 60870-5-104 Protocol. *Energy Informatics*, *3*(Suppl 1), 2–17. https://doi.org/10.1186/s42162-020-00118-4

Fichera, S., Galluccio, L., Grancagnolo, S. C., Morabito, G., & Palazzo, S. (2015). OPERETTA: An OPEnflow-based REmedy to mitigate TCP SYNFLOOD Attacks against web servers. *Computer Networks*, *92*, 89–100. https://doi.org/10.1016/j.comnet.2015.08.038

Gadze, J. D., Bamfo-Asante, A. A., Agyemang, J. O., Nunoo-Mensah, H., & Opare, K. A.-B. (2021). An Investigation into the Application of Deep Learning in the Detection and Mitigation of DDOS Attack on SDN Controllers. *Technologies*, *9*(1), 14. https://doi.org/10.3390/technologies9010014

Gao, W., Morris, T., Reaves, B., & Richey, D. (2010). On SCADA control system command and response injection and intrusion detection. *General Members Meeting and ECrime Researchers Summit, ECrime 2010*. https://doi.org/10.1109/ecrime.2010.5706699

Ghanem, W. A. H. M., Jantan, A., Ghaleb, S. A. A., & Nasser, A. B. (2020). An Efficient Intrusion Detection Model Based on Hybridization of Artificial Bee Colony and Dragonfly Algorithms for Training Multilayer Perceptrons. *IEEE Access*, *8*, 130452–130475. https://doi.org/10.1109/ACCESS.2020.3009533

Gogoi, P., Bhattacharyya, D. K., Borah, B., & Kalita, J. K. (2011). A survey of outlier detection methods in network anomaly identification. *Computer Journal*, *54*(4), 570–588. https://doi.org/10.1093/comjnl/bxr026

Grammatikis, P. R., Sarigiannidis, P., Sarigiannidis, A., Margounakis, D.,

Tsiakalos, A., & Efstathopoulos, G. (2020). An Anomaly Detection Mechanism for IEC 60870-5-104. *2020 9th International Conference on Modern Circuits and Systems Technologies, MOCAST 2020*, 0–3. https://doi.org/10.1109/MOCAST49295.2020.9200285

Gumaei, A., Hassan, M. M., Huda, S., Hassan, M. R., Camacho, D., Del Ser, J., & Fortino, G. (2020). A robust cyberattack detection approach using optimal features of SCADA power systems in smart grids. *Applied Soft Computing Journal*, *96*(November 2020), 1–17. https://doi.org/10.1016/j.asoc.2020.106658

Gupta, N., Jindal, V., & Bedi, P. (2021). LIO-IDS: Handling class imbalance using LSTM and improved one-vs-one technique in intrusion detection system. *Computer Networks*, *192*(March), 1–19. https://doi.org/10.1016/j.comnet.2021.108076

Hahn, A., Sun, C.-C., & Liu, C.-C. (2016). Cybersecurity of SCADA within Substations. *Smart Grid Handbook*, 1–17. https://doi.org/10.1002/9781118755471.sgd055

Hamid, Y., Shah, F. A., & Sugumaran, M. (2019). Wavelet neural network model for network intrusion detection system. *International Journal of Information Technology (Singapore)*, *11*(2), 251–263. https://doi.org/10.1007/s41870-018-0225-x

Hartpence, B., & Kwasinski, A. (2020). Combating TCP Port Scan Attacks Using Sequential Neural Networks. *2020 International Conference on Computing, Networking and Communications, ICNC 2020*, 256–260. https://doi.org/10.1109/ICNC47757.2020.9049730

Hilda, M., Louk, L., & Adhi, B. (2023). Dual-IDS : A bagging-based gradient boosting decision tree model for network anomaly intrusion detection system. *Expert Systems With Applications*, *213*(PB), 119030. https://doi.org/10.1016/j.eswa.2022.119030

Hindy, H., Brosset, D., Bayne, E., Seeam, A. K., Tachtatzis, C., Atkinson, R., & Bellekens, X. (2020). A Taxonomy of Network Threats and the Effect of Current Datasets on Intrusion Detection Systems. *IEEE Access*, *8*, 104650–104675. https://doi.org/10.1109/ACCESS.2020.3000179

Hodo, E., Grebeniuk, S., Ruotsalainen, H., & Tavolato, P. (2017). Anomaly detection for simulated IEC-60870-5-104 traffic. *ACM International Conference Proceeding Series*, *Part F1305*, 1–7. https://doi.org/10.1145/3098954.3103166

Hossain, M. S., Rahman, M., Sarker, M. T., Haque, M. E., & Jahid, A. (2019). A smart IoT based system for monitoring and controlling the sub-station equipment. *Internet of Things*, *7*, 100085. https://doi.org/10.1016/j.iot.2019.100085

Hou, W., Zhang, X., Guo, L., Sun, Y., Wang, S., & Zhang, Y. (2016). Taxonomy of attacks on Industrial Control protocols. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, *9784*, 78–87. https://doi.org/10.1007/978-3-319-42553-5_7

Imrana, Y., Xiang, Y., Ali, L., & Abdul-Rauf, Z. (2021). A bidirectional LSTM

deep learning approach for intrusion detection. *Expert Systems with Applications*, *185*(June 2020), 1–12. https://doi.org/10.1016/j.eswa.2021.115524

Irmak, E., & Erkek, I. (2018). An overview of cyber-attack vectors on SCADA systems. *6th International Symposium on Digital Forensic and Security, ISDFS 2018 - Proceeding*, *2018-Janua*, 1–5. https://doi.org/10.1109/ISDFS.2018.8355379

Jiawei Han, Jian Pei, M. K. (2011). Data mining: Data mining concepts and techniques. In *Elsevier*. https://doi.org/10.1109/ICMIRA.2013.45

Jin, F., Chen, M., Zhang, W., Yuan, Y., & Wang, S. (2021). Intrusion detection on internet of vehicles via combining log-ratio oversampling, outlier detection and metric learning. *Information Sciences*, *579*, 814–831. https://doi.org/10.1016/j.ins.2021.08.010

Kalech, M. (2019). Cyber-attack detection in SCADA systems using temporal pattern recognition techniques. *Computers and Security*, *84*, 225–238. https://doi.org/10.1016/j.cose.2019.03.007

Khalid, S., Khalil, T., & Nasreen, S. (2014). A survey of feature selection and feature extraction techniques in machine learning. *Proceedings of 2014 Science and Information Conference, SAI 2014*, 372–378. https://doi.org/10.1109/SAI.2014.6918213

Khan, I. A., Pi, D., Khan, Z. U., Hussain, Y., & Nawaz, A. (2019). Hml-ids: A hybrid-multilevel anomaly prediction approach for intrusion detection in scada systems. *IEEE Access*, *7*, 89507–89521. https://doi.org/10.1109/ACCESS.2019.2925838

Kumar, M. S., Ben-Othman, J., Srinivasagan, K. G., & Krishnan, G. U. (2019). Artificial Intelligence Managed Network Defense System against Port Scanning Outbreaks. *Proceedings - International Conference on Vision Towards Emerging Trends in Communication and Networking, ViTECoN 2019*, 1–5. https://doi.org/10.1109/ViTECoN.2019.8899380

Kwon, Y. J., Kim, H. K., Lim, Y. H., & Lim, J. I. (2015). A behavior-based intrusion detection technique for smart grid infrastructure. *2015 IEEE Eindhoven PowerTech, PowerTech 2015*. https://doi.org/10.1109/PTC.2015.7232339

Lin, C., & Nadjm-tehrani, S. (n.d.). Timing Patterns and Correlations in Spontaneous SCADA Traffic for Anomaly Detection. *Raid 2019*, 73–88.

Lin, C. Y., Fundin, A., Westring, E., Gustafsson, T., & Nadim-Tehrani, S. (2021). RICSel21 Data Collection: Attacks in a Virtual Power Network. *2021 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids, SmartGridComm 2021*, 201–206. https://doi.org/10.1109/SmartGridComm51999.2021.9632328

Lin, C. Y., & Nadjm-Tehrani, S. (2018). Understanding IEC-60870-5-104 traffic patterns in SCADA networks. *CPSS 2018 - Proceedings of the 4th ACM Workshop on Cyber-Physical System Security, Co-Located with ASIA CCS 2018*, 51–60. https://doi.org/10.1145/3198458.3198460

Linda, O., Vollmer, T., & Manic, M. (2009). Neural Network based intrusion detection system for critical infrastructures. *Proceedings of the International*

Joint Conference on Neural Networks, 1827–1834. https://doi.org/10.1109/IJCNN.2009.5178592

Liu, G., Zhao, H., Fan, F., Liu, G., Xu, Q., & Nazir, S. (2022). An Enhanced Intrusion Detection Model Based on Improved kNN in WSNs. *Sensors*, *22*(4), 1–18. https://doi.org/10.3390/s22041407

Lopez Perez, R., Adamsky, F., Soua, R., & Engel, T. (2018). Machine Learning for Reliable Network Attack Detection in SCADA Systems. *Proceedings - 17th IEEE International Conference on Trust, Security and Privacy in Computing and Communications and 12th IEEE International Conference on Big Data Science and Engineering, Trustcom/BigDataSE 2018*, 633–638. https://doi.org/10.1109/TrustCom/BigDataSE.2018.00094

Lopez Perez, R., Adamsky, F., Soua, R., & Engel, T. (2019). Forget the Myth of the Air Gap: Machine Learning for Reliable Intrusion Detection in SCADA Systems. *ICST Transactions on Security and Safety*, *6*(19), 159348. https://doi.org/10.4108/eai.25-1-2019.159348

Maglaras, L. A., & Jiang, J. (2014). Intrusion detection in SCADA systems using machine learning techniques. *Proceedings of 2014 Science and Information Conference, SAI 2014*, 626–631. https://doi.org/10.1109/SAI.2014.6918252

Mai, K., Qin, X., Ortiz Silva, N., & Cardenas, A. A. (2019). IEC 60870-5-104 network characterization of a large-scale operational power grid. *Proceedings - 2019 IEEE Symposium on Security and Privacy Workshops, SPW 2019*, 236–241. https://doi.org/10.1109/SPW.2019.00051

Mašetić, Z., Kečo, D., Doğru, N., & Hajdarević, K. (2017). SYN flood attack detection in cloud computing using support vector machine. *TEM Journal*, *6*(4), 752–759. https://doi.org/10.18421/TEM64-15

Maynard, P., & McLaughlin, K. (2020). *Towards Understanding Man-on-the-Side Attacks (MotS) in SCADA Networks*. https://doi.org/10.5220/0009782302870294

Maynard, P., McLaughlin, K., & Haberler, B. (2014). *Towards Understanding Man-In-The-Middle Attacks on IEC 60870-5-104 SCADA Networks*. 30–42. https://doi.org/10.14236/ewic/ics-csr2014.5

Maynard, P., McLaughlin, K., & Sezer, S. (2018). An Open Framework for Deploying Experimental SCADA Testbed Networks. *Ics-Csr 2018*, *2018*, 89–98. https://doi.org/10.14236/ewic/ics2018.11

Mohammadi, M., Rashid, T. A., Karim, S. H. T., Aldalwie, A. H. M., Tho, Q. T., Bidaki, M., Rahmani, A. M., & Hosseinzadeh, M. (2021). A comprehensive survey and taxonomy of the SVM-based intrusion detection systems. *Journal of Network and Computer Applications*, *178*(December 2020), 102983. https://doi.org/10.1016/j.jnca.2021.102983

Nicholas R. Rodofile1(B), Thomas Schmidt1, 2, Sebastian T. Sherry1, Christopher Djamaludin1, Kenneth Radke1, and E. F. (2017). *Process Control Cyber-Attacks and Labelled Datasets on S7Comm Critical Infrastructure*. *1*, 406–413. https://doi.org/10.1007/978-3-319-59870-3

Oliveira, N., Praça, I., Maia, E., & Sousa, O. (2021). Intelligent cyber attack detection and classification for network-based intrusion detection systems. *Applied Sciences (Switzerland)*, *11*(4), 1–21.

https://doi.org/10.3390/app11041674

Ortega, A., Schweitzer, C. M., Shinoda, A. A., & Ortega, A. V. (2017). Simulation of the DNP3 protocol over TCP/IP on a network IEEE 802.11g ad-hoc with smart meter. *Proceedings of the 2016 IEEE ANDESCON, ANDESCON 2016*, *October*, 0–4. https://doi.org/10.1109/ANDESCON.2016.7836213

Panesar, A., & Panesar, A. (2016). Machine Learning Algorithms. *Machine Learning and AI for Healthcare*, 1–152. https://doi.org/10.1007/978-1-4842-3799-1_4

Petr, M. (2017). *Description and analysis of IEC 104 Protocol*. http://www.fit.vutbr.cz/~matousp/grants.php.en?id=1101.

Pliatsios, D., Sarigiannidis, P., Lagkas, T., & Sarigiannidis, A. G. (2020). A Survey on SCADA Systems: Secure Protocols, Incidents, Threats and Tactics. *IEEE Communications Surveys and Tutorials*, *22*(3), 1942–1976. https://doi.org/10.1109/COMST.2020.2987688

priyadarsini, P. I. (2021). ABC-BSRF: Artificial Bee Colony and Borderline-SMOTE RF Algorithm for Intrusion Detection System on Data Imbalanced Problem. In *Lecture Notes on Data Engineering and Communications Technologies* (Vol. 56). Springer Singapore. https://doi.org/10.1007/978-981-15-8767-2_2

Puri, A., & Gupta, M. K. (2019). Comparative Analysis of Resampling Techniques under Noisy Imbalanced Datasets. *IEEE International Conference on Issues and Challenges in Intelligent Computing Techniques, ICICT 2019*. https://doi.org/10.1109/ICICT46931.2019.8977650

Qaddoura, R., Al-Zoubi, A. M., Almomani, I., & Faris, H. (2021). A multi-stage classification approach for iot intrusion detection based on clustering with oversampling. *Applied Sciences (Switzerland)*, *11*(7). https://doi.org/10.3390/app11073022

Qian, J., Du, X., Chen, B., Qu, B., Zeng, K., & Liu, J. (2020). Cyber-Physical Integrated Intrusion Detection Scheme in SCADA System of Process Manufacturing Industry. *IEEE Access*, *8*, 147471–147481. https://doi.org/10.1109/ACCESS.2020.3015900

Radoglou-Grammatikis, P., Sarigiannidis, P., Efstathopoulos, G., Karypidis, P. A., & Sarigiannidis, A. (2020). DIDEROT: An intrusion detection and prevention system for DNP3-based SCADA systems. *ACM International Conference Proceeding Series*. https://doi.org/10.1145/3407023.3409314

Radoglou-Grammatikis, P., Sarigiannidis, P., Giannoulakis, I., Kafetzakis, E., & Panaousis, E. (2019). *Attacking IEC-60870-5-104 SCADA Systems*. *June*, 41–46. https://doi.org/10.1109/services.2019.00022

Rajasegarar, S., Leckie, C., & Palaniswami, M. (2014). Hyperspherical cluster based distributed anomaly detection in wireless sensor networks. *Journal of Parallel and Distributed Computing*, *74*(1), 1833–1847. https://doi.org/10.1016/j.jpdc.2013.09.005

Reza, M. S., & Ma, J. (2016). ICA and PCA integrated feature extraction for classification. *International Conference on Signal Processing Proceedings, ICSP*, *0*, 1083–1088. https://doi.org/10.1109/ICSP.2016.7877996

Robles-Durazno, A., Moradpoor, N., McWhinnie, J., & Russell, G. (2018). A

supervised energy monitoring-based machine learning approach for anomaly detection in a clean water supply system. *2018 International Conference on Cyber Security and Protection of Digital Services, Cyber Security 2018*, 1–8. https://doi.org/10.1109/CyberSecPODS.2018.8560683

Rodofile, N. R., Radke, K., & Foo, E. (2017). Framework for SCADA cyber-attack dataset creation. *ACM International Conference Proceeding Series*, 1–10. https://doi.org/10.1145/3014812.3014883

Roldán, J., Boubeta-Puig, J., Luis Martínez, J., & Ortiz, G. (2020). Integrating complex event processing and machine learning: An intelligent architecture for detecting IoT security attacks. *Expert Systems with Applications*, *149*. https://doi.org/10.1016/j.eswa.2020.113251

Rubio, J. E., Alcaraz, C., Roman, R., & Lopez, J. (2019). Current cyber-defense trends in industrial control systems. *Computers and Security*, *87*, 101561. https://doi.org/10.1016/j.cose.2019.06.015

Samtani, S., Yu, S., Zhu, H., Patton, M., & Chen, H. (2016). Identifying SCADA vulnerabilities using passive and active vulnerability assessment techniques. *IEEE International Conference on Intelligence and Security Informatics: Cybersecurity and Big Data, ISI 2016*, 25–30. https://doi.org/10.1109/ISI.2016.7745438

Samtani, S., Yu, S., Zhu, H., Patton, M., Matherly, J., & Chen, H. C. (2018). Identifying Supervisory Control and Data Acquisition (SCADA) Devices and their Vulnerabilities on the Internet of Things (IoT): A Text Mining Approach. *IEEE Intelligent Systems, 2018.*, 1–11. https://doi.org/10.1109/MIS.2018.111145022

Seo, J. H., & Kim, Y. H. (2018). Machine-learning approach to optimize smote ratio in class imbalance dataset for intrusion detection. *Computational Intelligence and Neuroscience*, *2018*. https://doi.org/10.1155/2018/9704672

Shafique, H., Shah, A. A., Qureshi, M. A., & Ehsan, M. K. (2022). Machine Learning Empowered Efficient Intrusion Detection Framework. *VFAST Transactions on Software Engineering*, *10*(2), 27–35. https://doi.org/http://dx.doi.org/10.21015/vtse.v10i2.1017

Sharmila, B. S., & Nagapadma, R. (2019). Intrusion detection system using naive bayes algorithm. *2019 5th IEEE International WIE Conference on Electrical and Computer Engineering, WIECON-ECE 2019 - Proceedings*, 8–11. https://doi.org/10.1109/WIECON-ECE48653.2019.9019921

Shi, S., Wang, Y., Zou, C., & Tian, Y. (2022). AES RSA-SM2 Algorithm against Man-in-the-Middle Attack in IEC 60870-5-104 Protocol. *Journal of Computer and Communications*, *10*(01), 27–41. https://doi.org/10.4236/jcc.2022.101002

Shosha, A. F., Gladyshev, P., Wu, S. S., & Liu, C. C. (2011). Detecting cyber intrusions in SCADA networks using multi-agent collaboration. *2011 16th International Conference on Intelligent System Applications to Power Systems, ISAP 2011*, 1–7. https://doi.org/10.1109/ISAP.2011.6082170

Somvanshi, M., Chavan, P., Tambade, S., & Shinde, S. V. (2017). A review of machine learning techniques using decision tree and support vector machine. *Proceedings - 2nd International Conference on Computing, Communication, Control and Automation, ICCUBEA 2016*.

https://doi.org/10.1109/ICCUBEA.2016.7860040

Suaboot, J., Fahad, A., Tari, Z., Grundy, J., Mahmood, A. N., Almalawi, A., Zomaya, A. Y., & Drira, K. (2020). A Taxonomy of Supervised Learning for IDSs in SCADA Environments. *ACM Computing Surveys*, *53*(2). https://doi.org/10.1145/3379499

Sverko, M., Grbac, T. G., & Mikuc, M. (2022). Supervisory Control and Data Acquisition (SCADA) Systems in Continuous Manufacturing Process Control (Focus on Steel Industry). *IEEE Access*, *10*(September), 109395–109430. https://doi.org/10.1109/ACCESS.2022.3211288

Tahir, M., Li, M., Ayoub, N., Shehzaib, U., & Wagan, A. (2018). A Novel DDoS floods detection and testing approaches for network traffic based on Linux Techniques. *International Journal of Advanced Computer Science and Applications*, *9*(2), 341–357. https://doi.org/10.14569/IJACSA.2018.090248

Tan, X., Su, S., Huang, Z., Guo, X., Zuo, Z., Sun, X., & Li, L. (2019). Wireless sensor networks intrusion detection based on SMOTE and the random forest algorithm. *Sensors (Switzerland)*, *19*(1). https://doi.org/10.3390/s19010203

Teixeira, M. A., Salman, T., Zolanvari, M., Jain, R., Meskin, N., & Samaka, M. (2018). SCADA system testbed for cybersecurity research using machine learning approach. *Future Internet*, *10*(8). https://doi.org/10.3390/fi10080076

Texas, C. E. (2012). BLOOM FILTER BASED INTRUSION DETECTION FOR SMART GRID SCADA. *Saranya Parthasarathy, Deepa Kundur*, *May*.

Ullah, I., & Mahmoud, Q. H. (2018). A hybrid model for anomaly-based intrusion detection in SCADA networks. *Proceedings - 2017 IEEE International Conference on Big Data, Big Data 2017*, *2018-Janua*, 2160–2167. https://doi.org/10.1109/BigData.2017.8258164

Upadhyay, D., Manero, J., Zaman, M., & Sampalli, S. (2021a). Intrusion Detection in SCADA Based Power Grids: Recursive Feature Elimination Model with Majority Vote Ensemble Algorithm. *IEEE Transactions on Network Science and Engineering*, *8*(3), 2559–2574. https://doi.org/10.1109/TNSE.2021.3099371

Upadhyay, D., Manero, J., Zaman, M., & Sampalli, S. (2021b). Learning Classifiers for Intrusion Detection on Power Grids. *IEEE TRANSACTIONS ON NETWORK AND SERVICE MANAGEMENT*, *18*(1), 1104–1116.

Volkova, A., Niedermeier, M., Basmadjian, R., & De Meer, H. (2019). Security challenges in control network protocols: A survey. *IEEE Communications Surveys and Tutorials*, *21*(1), 619–639. https://doi.org/10.1109/COMST.2018.2872114

Waagsnes, H., & Ulltveit-Moe, N. (2018). Intrusion detection system test framework for SCADA systems. *ICISSP 2018 - Proceedings of the 4th International Conference on Information Systems Security and Privacy*, *2018-Janua*(Icissp), 275–285. https://doi.org/10.5220/0006588202750285

Wang, J. H., & Septian, T. W. (2021). Combining Oversampling with Recurrent Neural Networks for Intrusion Detection. In *Database Systems for Advanced Applications: Vol. 12680 LNCS* (pp. 305–320). https://doi.org/10.1007/978-3-030-73216-5_21

Wang, X., & Foo, E. (2018). Assessing Industrial Control System Attack Datasets

for Intrusion Detection. *2018 3rd International Conference on Security of Smart Cities, Industrial Control System and Communications, SSIC 2018 - Proceedings*, 1–8. https://doi.org/10.1109/SSIC.2018.8556706

Wang, Z., Li, Z., He, D., & Chan, S. (2022). A lightweight approach for network intrusion detection in industrial cyber-physical systems based on knowledge distillation and deep metric learning. *Expert Systems with Applications*, *206*(May 2022), 1–17. https://doi.org/10.1016/j.eswa.2022.117671

Wankhede, S., & Kshirsagar, D. (2018). DoS Attack Detection Using Machine Learning and Neural Network. *Proceedings - 2018 4th International Conference on Computing, Communication Control and Automation, ICCUBEA 2018*. https://doi.org/10.1109/ICCUBEA.2018.8697702

Wu, T., Fan, H., Zhu, H., You, C., Zhou, H., & Huang, X. (2022). Intrusion detection system combined enhanced random forest with SMOTE algorithm. *Eurasip Journal on Advances in Signal Processing*, *2022*(1). https://doi.org/10.1186/s13634-022-00871-6

Yadav, G., & Paul, K. (2021). Architecture and security of SCADA systems: A review. *International Journal of Critical Infrastructure Protection*, *34*, 100433. https://doi.org/10.1016/j.ijcip.2021.100433

Yang, H., Cheng, L., & Chuah, M. C. (2019). Deep-Learning-Based Network Intrusion Detection for SCADA Systems. *2019 IEEE Conference on Communications and Network Security, CNS 2019*, 1–7. https://doi.org/10.1109/CNS.2019.8802785

Yang, Y., McLaughlin, K., Littler, T., Sezer, S., Pranggono, B., & Wang, H. F. (2013). Intrusion Detection System for IEC 60870-5-104 based SCADA networks. *IEEE Power and Energy Society General Meeting*. https://doi.org/10.1109/PESMG.2013.6672100

Yang, Y., Xu, H. Q., Gao, L., Yuan, Y. B., McLaughlin, K., & Sezer, S. (2017). Multidimensional Intrusion Detection System for IEC 61850-Based SCADA Networks. *IEEE Transactions on Power Delivery*, *32*(2), 1068–1078. https://doi.org/10.1109/TPWRD.2016.2603339

Yoo, H., & Shon, T. (2016). Challenges and research directions for heterogeneous cyber-physical system based on IEC 61850: Vulnerabilities, security requirements, and security architecture. *Future Generation Computer Systems*, *61*, 128–136. https://doi.org/10.1016/j.future.2015.09.026

Zhang, H., Huang, L., Wu, C. Q., & Li, Z. (2020). An effective convolutional neural network based on SMOTE and Gaussian mixture model for intrusion detection in imbalanced dataset. *Computer Networks*, *177*(April). https://doi.org/10.1016/j.comnet.2020.107315

Zhang, J., Gan, S., Liu, X., & Zhu, P. (2016). Intrusion detection in SCADA systems by traffic periodicity and telemetry analysis. *Proceedings - IEEE Symposium on Computers and Communications*, *2016-Augus*, 318–325. https://doi.org/10.1109/ISCC.2016.7543760

Zhang, Y., Meratnia, N., & Havinga, P. (2010). Outlier detection techniques for wireless sensor networks: A survey. *IEEE Communications Surveys and Tutorials*, *12*(2), 159–170. https://doi.org/10.1109/SURV.2010.021510.00088

Zolanvari, M., Teixeira, M. A., Gupta, L., Khan, K. M., & Jain, R. (2019). Machine

Learning-Based Network Vulnerability Analysis of Industrial Internet of Things. *IEEE Internet of Things Journal*, *6*(4), 6822–6834. https://doi.org/10.1109/JIOT.2019.2912022

Zuech, R., Hancock, J., & Khoshgoftaar, T. M. (2021). Detecting web attacks using random undersampling and ensemble learners. *Journal of Big Data*, *8*(1). https://doi.org/10.1186/s40537-021-00460-8