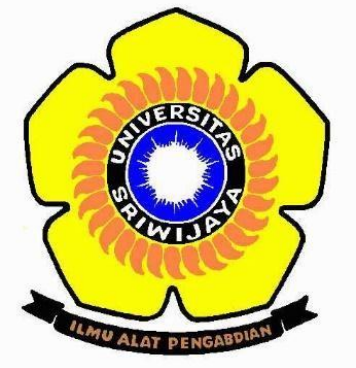
DETEKSI SERANGAN *MAN IN THE MIDDLE* (MITM) *ATTACK* PADA JARINGAN *SUPERVISORY CONTROL AND DATA ACQUISITION* (SCADA) MENGGUNAKAN *RANDOM FOREST*

TUGAS AKHIR

Diajukan Untuk Melengkapi Salah Satu Syarat
Memperoleh Gelar Sarjana Komputer



Oleh :

SERGIO SEPTIANO
09011181621015

JURUSAN SISTEM KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS SRIWIJAYA
2021

LEMBAR PENGESAHAN

DETEKSI SERANGAN *MAN IN THE MIDDLE* (MITM) *ATTACK* PADA JARINGAN *SUPERVISORY CONTROL AND DATA ACQUISITION* (SCADA) MENGGUNAKAN *RANDOM FOREST*

TUGAS AKHIR

Diajukan Untuk Melengkapi Salah Satu Syarat
Memperoleh Gelar Sarjana Komputer

Oleh :
SERGIO SEPTIANO
09011181621015

Indralaya, April 2021

Pembimbing I,	Pembimbing II,
Deris Stiawan, M.T., Ph.D.	**Ahmad Heryanto, S.Kom. M.T.**
NIP. 197806172006041002	**NIP. 198701222015041002**

Mengetahui,
Ketua Jurusan Sistem Komputer

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

HALAMAN PERSETUJUAN

Telah diuji dan lulus pada:

Hari : **Rabu**

Tanggal : **14 April 2021**

Tim Penguji:

1. **Ketua** : **Sarmayanta Sembiring, S.SI., M.T**
2. **Penguji** : **Huda Ubaya, S.T., M.T.**

Mengtahui,

Ketua Jurusan Sistem Komputer

Dr. Ir. Sukemi, M.T.

NIP. 196612032006041001

HALAMAN PERNYATAAN

Yang bertanda tangan dibawah ini:

Nama : **Sergio Septiano**

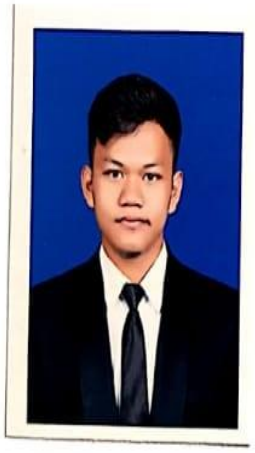
NIM : **09011181621015**

Judul : **Deteksi Serangan *Man In The Middle* Pada Jaringan Scada Menggunakan Random Forest**

Hasil Pengecekan Software iThenticate/Turnitin : 13 %

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

Demikian, Pernyataan ini saya buat dalam keadaan sadar dan tidak dipaksakan.



Palembang, Juni 2021

Sergio Septiano

NIM. 09011181621015

HALAMAN PERSEMBAHAN

“Allah tidak membebani seseorang melainkan sesuai dengan kesanggupannya”

(*Q.S Al-Baqarah 2:286*)

“You’ll Never Walk Alone”

Tugas Akhir ini kupesembahkan untuk:

- Ibunda Masayu Mardaleni dan Ayahanda Joni Ismail atas segala doa dan dukungan kepada putranya dalam menyelesaikan studinya.
- Seluruh keluarga yang berperan khususnya kakakku Arles Mana Suparja yang selalu mendukungku.
- Dosen pembimbing terbaik yang pernah ada, Bapak Deris Stiawan M.T., Ph.D. dan Bapak Ahmad Heryanto S.Kom., M.T.
- Teman-teman seperjuangan khususnya teman riset Scada, Kak Wanda,Yogi, dan Harry,Farhan, dan yang lainnya.
- Teman- teman LTS Ori yang selalu memberikan dukungan dan hiburan di saaat susah.
- Almamater.

KATA PENGANTAR

Puji dan syukur kepada Allah SWT, atas limpahan rahmat dan karunia-Nya yang telah memberikan penulis kesehatan dan kesempatan sebaik-baiknya, sehingga penulis dapat merampungkan Tugas Akhir in dengan judul "Deteksi *Man In The Middle* (MITM) Attack pada jaringan *Supervisory Control And Data Acquisition* (SCADA) menggunakan *Random Fore*st "**.** Penulisan Tugas Akhir ini dilakukan untuk melengkapi salah satu syarat memperoleh gelar Sarjana Komputer di Jurusan Sistem Komputer Fakultas Ilmu Komputer Universitas Sriwijaya. Pada kesempatan ini juga, penulis menyampaikan ucapan terima kasih yang sebesar-besarnya kepada semua pihak yang telah membantu baik dari segi moril ataupun materil serta memberikan kemudahan, dorongan, saran dan kritik selama dalam proses penulisan Tugas Akhir ini. Oleh karena itu, pada kesempatan ini penulis mengucapkan rasa syukur kepada Allah SWT. dan mengucapkan terima kasih kepada yang terhormat :

1. Ayah handa Joni Ismail dan ibunda yang kusayangi Masayu Mardaleni serta keluarga penulis tercinta, yang telah mencurahkan segenap cinta dan kasih sayang serta perhatian moril maupun materil kepada penulis selama melaksanakan dan mengikuti perkuliahan di Jurusan Sistem Komputer Fakultas Ilmu Komputer Universitas Sriwijaya, semoga Allah SWT selalu melindungi, melimpahkan rahmat, kesehatan, karunia dan keberkahan di dunia maupun di akhirat atas budi baik yang telah diberikan kepada penulis.
2. Bapak Jaidan Jauhari, S.Pd., M.T., selaku Dekan Fakultas Ilmu Komputer Universitas Sriwijaya.
3. Bapak Dr. Ir. H. Sukemi, M.T., selaku Ketua Jurusan Sistem Komputer Fakultas Ilmu Komputer Universitas Sriwijaya.
4. DR. Erwin, S.SI, M.SI selaku Dosen Pembimbing Akademik di Jurusan Sistem Komputer Fakultas Ilmu Komputer Universitas Sriwijaya.
5. Bapak Deris Stiawan, M.T., Ph.D. selaku Dosen Pembimbing I Tugas Akhir di Jurusan Sistem Komputer Fakultas Ilmu Komputer Universitas Sriwijaya.

6. Bapak Ahmad Heryanto, S.Kom,. M.T. selaku Dosen Pembimbing II Tugas Akhir di jurusan Sistem Komputer Fakultas Ilmu Komputer Universitas Sriwijaya.
7. Mbak Renny selaku admin Jurusan Sistem Komputer yang telah membantu mengurus seluruh berkas.
8. Seluruh dosen, staff, serta karyawan Fakultas Ilmu Komputer Universitas Sriwijaya.
9. Seluruh teman-teman seperjuangan angkatan 2016 Sistem Komputer Fakultas Ilmu Komputer Universitas Sriwijaya.
10. Almamaterku.

Akhir kata penulis menyadari bahwa dalam penulisan Proposal Tugas Akhir ini masih jauh dari kesempurnaan. Oleh karena itu, penulis memohon saran dan kritik yang sifatnya membangun demi kesempurnaan Proposal Tugas Akhir ini dan semoga bermanfaat bagi kita semua baik dalam dunia Pendidikan maupun dalam lingkungan masyarakat. Aamiin.

Indralaya, April 2021
Penulis

Sergio Septiano
Nim. 09011181621015

DETEKSI SERANGAN *MAN IN THE MIDLE PADA JARINGAN SUPERVISORY CONTROL AND DATA ACQUISTION MENGGUNAKAN RANDOM FOREST*

Sergio Septiano (0901181621015)

Jurusan Sistem Komputer, Fakultas Ilmu Komputer, Universitas Sriwijaya

Email : septiano96sergio@gmail.com

ABSTRAK

Supervisory Control and Data Acquisition (SCADA) merupakan suatu sistem di industri digunakan untuk mengontrol perangkat dari jarak jauh dengan jaringan computer. Salah satu protokol dari SCADA adalah IEC 104 yang berbasis TCP IP. Protokol ini memiliki kerentanan karena pada protokol ini data yang dikirim tidak dienkripsi yang memungkintan serangan *Man In The Middle* (MITM) dapat dilakukan. ARP Spoofing merupakan salah satu serangan MITM yang dapat dilakukan dengan menyamar cara melalui mac dan ip address korban. Penggunaan metode *Intrusion Detection System* (IDS) untuk mendeteksi paket yang ada terdapat serangan atau tidak dengan menggunakan Snort IDS,untuk mengetahui pola serangan yang ada. Klasifikasi menggunakan *Random Forest* digunakan untuk membedakan antara paket normal dan serangan. Hasil terbaik dari Algoritma *Random Forest* dengan evaluasi confusion matrix didapatkan akurasi terbaik sebesar 99.93%, serta nilai *OOB Score* sebesar 0.07% dan nilai *Un-Detection Rate* sebesar 0.05%.

Kata kunci: *Supervisory Control And Data Acquisition, Man In The Middle, Instrusion Detection System, Confusion Matrix.*

Mengetahui

Pembimbing I	**Pembimbing II**
Deris Stiawan, Ph.D.	**Ahmad Heryanto,S.Kom.,M.T**
NIP. 197806172006041002	**NIP.198701222015041002**

Ketua Jurusan Sistem Komputer

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

NIP. 196612032006041001

DETECTION OF MAN IN THE MIDDLE ATTACK ON NETWORK SUPERVISORY CONTROL AND DATA ACQUISITION USING RANDOM FOREST

Sergio Septiano (0901181621015)

Department of Computer Systems, Faculty of Computer Science,

Sriwijaya University

Email : septiano96sergio@gmail.com

ABSTRACT

Supervisory Control and Data Acquisition (SCADA) is a system in industry used to control devices remotely with a computer network. One of the protocols from SCADA is IEC 104 which is based on TCP IP. This protocol has a vulnerability because in this protocol the data sent is not encrypted which allows Man In The Middle (MITM) attacks to be carried out. ARP Spoofing is one of the MITM attacks that can be done by impersonating the victim's MAC and IP address. The use of the Intrusion Detection System (IDS) method to detect packets that have an attack or not by using Snort IDS, to find out existing attack patterns. Classification using Random Forest is used to differentiate between normal and attack packets. The best results of the Random Forest Algorithm with the evaluation of the confusion matrix obtained the best accuracy of 99.93%, as well as the OOB Score value of 0.07% and the Un-Detection Rate value of 0.05%..

Keywords: *Supervisory Control And Data Acquisition, Man In The Middle, Instrusion Detection System, Confusion Matrix.*

Mengetahui

Pembimbing I	**Pembimbing II**
Deris Stiawan, Ph.D.	**Ahmad Heryanto,S.Kom.,M.T**
NIP. 197806172006041002	**NIP.198701222015041002**

Ketua Jurusan Sistem Komputer

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

NIP. 196612032006041001

DAFTAR ISI

Halaman

DAFTAR GAMBAR

Halaman

DAFTAR TABEL

Halaman

DAFTAR RUMUS

Halaman

BAB I
PENDAHULUAN

1.1 Latar Belakang

Supervisory Control and Data Acquisition (SCADA) adalah suatu system kotrol yang memungkinkan pemantauan dan pengelolaan proses industry dari jarak jauh dan kendalikan dengan memanfaatkan jaringan computer [1]. Sistem Scada sekarang telah menjadi sesuatu yang sangat penting bagi banyak industri di seluruh dunia. Saat ini sistem Scada banyak mengatur infrastruktur yang kritis seperti jaringan listrik, system pengolahan air, pabrik besar, sistem pengolahan air, dan bahkan tenaga nuklir [2]. Evolusi yang cepat dari layanan teknologi dan informasi telah mengubah jaringan listrik konvensional menjadi paradigma baru yang disebut *Smart Grid* (SG). Smart Grid membawa perbaikan yang signifikan ,seperti peningkatan keandalan dan manajemen energy yang lebih baik ,tetapi juga membawa tantangan keamanan di dalamnya. Salah satu alasan utama untuk ini adalah bahwa SG menggabungkan berbagai teknologi heterogen,termasuk perangkat *Internet of Things* (IoT) serta *Supervisory Control and Data Acquisition* (SCADA) *system* [3]. Dengan besarnya fungsi dari sistem Scada ini membuat sistem Scada menjadi target yang sangat menarik untuk serangan jahat *cyber*. Bagian yang rentan dari sistem Scada ini adalah pada protokol komunikasinya, yang memungkinkan serangan cyber seperti Denial of Service (DoS), Man In The Middle (MITM),dan Replay dapat dilakukan [2].

Serangan *Man In The Middle* (MITM) adalah salah satu ancaman yang terkenal dalam keamanan komputer. Dengan bertemunya antara perangkat pintar dan dan internet (internet of things) telah meningkatkan kebutuhan akan kerahasiaan data,integritas,dan ketersediaan informasi[4]. Serangan MITM memungkinkan serangan penyerang untuk memantau pertukaran informasi antara dua pihak dengan mengarahkan lalu lintas antara penyerang dan korban melewati mesin penyerang.[5]. Sebagian besar skema yang ada untuk menemukan MITM fokus serangan pada mendeteksi mekanisme yang digunakan untuk mengarahkan lalu lintas melalui mesin penyerang. Jenis serangan ini sangat berbahaya karena hampir tidak terlihat oleh korban. Serangan MITM bekerja sedemikian rupa

sehingga membuat pengguna sulit untuk memahami apakah mereka terhubung ke koneksi yang aman yang sebenarnya atau ke koneksi yang tidak aman serupa.

Pada sistem Scada terdapat beberapa protokol,salah satu protokol komunikasinya adalah protokol IEC-104. IEC-104 adalah protokol yang merupakan gabungan dari application message dari protokol IEC-101 dengan protokol TCP/IP. IEC-104 menambahkan transport layer dan network layer ke model *Enhanced Performance Architecture* (EPA) yang termasuk di application [6]. Peran *Intrusion Detection System* (IDS) sangat penting pada suatu jaringan computer.*Intrusion Detection System (IDS*) [7] adalah suatu mekanisme kemanan, yang dimana secara dinamis memonitoring,mencegah dan memblok intrusi sistem yang tidak normal. Dengan momonitor status dan perilaku maka IDS ini dapat mendeteksi dan menganalisis apakah pengguna system ini adalah normal ataupun tidak dan memanfaatkan celah kelemahan keamanan pada sistem dan mencoba melakukan serangan pada system.

P.Radoglou-Grammatikis et al pada penelitiannya, dilakukan pengujian terhadap kerentan keamanan protokol IEC-104 pada sistem Scada dengan melakukan 4 jenis serangan yang berbeda [3] . Masing-masing serangan tersebut adalah IEC-104 *Packet Flooding Attack*, TCP SYN DoS *Attack, Unauthorized Attack,* dan MiTM IEC 60870-5-104 *Isolation Attack*. Hasil dari pengujian menunjukkan bahwa *Unauthorized Attack* dan DoS *Attack* memiliki nilai resiko yang paling tinggi masing-masing 6.58 dan 6.06. Penilaian resiko yang digunakan berdasarkan *AlienVault's risk assessment model and real-world data values from the Common Weakness Enumeration* (CWE).

Pada penelitian lain L.Maglaras et al dengan penelitiannya [8] membahas mengenai IDS pada sistem Scada. Pada penelitiannya mereka menggunakan metode OSCVM (*One-Classs Support Vector Machine*) yang difungsikan untuk mendeteksi serangan pada jaringan Scada secara anomaly.Hasil dari pengujian menunjukkan bahwa model OSCVM memiliki akurasi sebesar 98.42% pada dataset A dengan 1000 *rows*, dan memiliki akurasi sebesar 99.12% pada dataset B dengan 570 *rows*, serta untuk split data A dan B memiliki akurasi sebesar 98.8796%.

Di penelitian lainnya [9] yang dilakukan oleh M.Teixeira et al, mereka melakukan uji coba IDS pada sistem Scada di lingkungan testbed yang mereka

rancang, yang kemudian dilakukan beberapa serangan pada protokol Modbus di lingkungan testbed tersebut dan dilakukan sistem deteksi dengan menggunakan beberapa metode tradisional *machine learning*. Salah satu metode yang mendapatkan hasil terbaik adalah metode *Random Forest* dengan akurasi sebesar 99.98% (*offline*) dan 99.89% (*online*), serta false alarm rate 0.01% (*offline*) dan 0% (*online*).

Pada penelitian ini akan membahas tentang bagaimana cara mendeteksi serangan Man In The Middle pada suatu jaringan industry SCADA pada protokol IEC-104. IDS ini akan menganalisis traffic/log dari suatu paket jaringan dan akan mengeluarkan suatu ouput yang biasa kita kenal sebagai *'alert'* sebagai tanda bahwa ada suatu kegiatan/perilaku yang tidak normal pada jaringan tersebut.. Pola yang tidak normal ini bisa kita deteksi dan anggap sebagai suatu serangan dengan menggunakan suatu teknologi yang bernama Machine Learning.

Algoritma pembelajaran mesin membangun model matematika berdasarkan data sampel,yang dikenal sebagai 'Data Training' untuk membuat prediksi atau suatu keputusan. Pada penelitian ini pendekatan machine learning yang digunakan adalah algoritma *Random Forest* [10]. Algoritma *Random Forest* terdiri dari kumpulan klasifikasi pohon terstruktur, dimana setiap pohon dibangun oleh sample bootsrap yang berbeda dari data asli menggunakan algoritma *decision tree*. Klasifikasi *Random Forest* dapat diperoleh dengan mengabil sampel suatu set atribut, kumpulan data, atau merubah beberapa parameter yang ada di dalam *decision tree*.

1.2 Perumusan Masalah

Berikut adalah rumusan masalah dalam penulisan Tugas Akhir ini:

1. Bagaimana cara mengekstrak data set ?
2. Apakah snort engine dapat mendeteksi pola serangan yang ada pada dataset*?*
3. Bagaimana pola serangan MITM yang didapatkan dari dataset?
4. Bagaimana performa *Random Forest* dalam mendeteksi dari pola serangan?

1.3 Tujuan Penelitian

Adapun tujuan tugas akhir ini adalah sebagai berikut:

1. Melakukan pengujian IDS dengan Snort engine menggunakan dataset.
2. Mampu mendeteksi pola serangan MITM.
3. Mengklasifikasikan serangan dengan metode *Random Forest*.

1.4 Manfaat Penelitian

Adapun manfaat tugas akhir ini adalah sebagai berikut:

1. Dapat mengetahui pola serangan pada dataset.
2. Dapat mencegah serangan MITM yang akan masuk ke sistem.
3. Dapat mengetahui performa dari metode yang digunakan dalam mengklasifikasikan paket normal dan serangan.

1.5 Batasan Masalah

Batasan masalah tugas akhir ini yaitu sebagai berikut:

1. Dalam penelitian ini serangan yang digunakan adalah *Arp Spoofing*.
2. Metode yang digunakan untuk mendeteksi serangan adalah *Random Forest*.
3. Menggunakan SMOTE untuk menyeimbangkan data kelas minoritas.
4. Menggunakan Dataset *Online* dari Situs Figshare.
5. Hanya mendeteksi dan mengenali serangan di protokol IEC104.
6. Bersifat *Offline*.

1.6 Sistematika Penulisan

Adapun sistematika dalam penulisan tugas akhir ini adalah sebagai berikut:

BAB1 Pendahuluan

Bab ini berisikan Latar Belakang penelitian tentang *Intrusion Detection System* (IDS) pada jaringan *Scada*, Perumusan Masalah yang ditemukan pada penelitian , Tujuan Penelitian *IDS* pada jaringan scada, Manfaat Penelitian *IDS* pada jaringan *Scada*, Batasan Masalah yang digunakan dalam pendeteksian serangan pada jaringan *Scada* dan Sistematika Penulisan.

BAB2 Tinjauan Pustaka

Bab ini akan berisi dasar teori dari SCADA, *Instrusion Detection System* (IDS),Protokol IEC104, *Snort* dan metode *Random Forest* yang berhubungan dengan penelitian,serta penggunaan *Smote* pada metode yang digunakan.

BAB3 Metodologi

Bab ini menjelaskan secara sistematis, bagaimana proses penelitian dilakukan. Dimulai dari perangkat yang digunakan dalam penelitian,lalu persiapan dataset yang diekstrak, melakukan *IDS* dengan *Snort*, dan deteksi serangan dengan menggunakan *Random Forest*.

BAB4 Hasil dan Analisis

Bab ini memiliki pembahasan mengenai pengekstrakan dataset, Tahap Pemrograman, Perbandingan Hasil Olah dan Dataset, Pengukuran Parameter, Pembahasan, dan Analisis.

BAB5 Kesimpulan dan Saran

Bab ini berisikan kesimpulan akhir atau hasil yang didapat dalam penelitian pendeteksian serangan *Arp Spoofing* pada jaringan *Scada*.

DAFTAR PUSTAKA

[1] A. F. S. Prisco and M. J. Freddy Duitama, "Intrusion detection system for SCADA platforms through machine learning algorithms," *2017 IEEE Colomb. Conf. Commun. Comput. COLCOM 2017 - Proc.*, pp. 1–6, 2017, doi: 10.1109/ColComCon.2017.8088210.

[2] N. Sayegh, A. Chehab, I. H. Elhajj, and A. Kayssi, "Internal security attacks on SCADA systems," *2013 3rd Int. Conf. Commun. Inf. Technol. ICCIT 2013*, pp. 22–27, 2013, doi: 10.1109/ICCITechnology.2013.6579516.

[3] P. Radoglou-Grammatikis, P. Sarigiannidis, I. Giannoulakis, E. Kafetzakis, and E. Panaousis, "Attacking IEC-60870-5-104 SCADA Systems," *Proc. - 2019 IEEE World Congr. Serv. Serv. 2019*, vol. 2642–939X, pp. 41–46, 2019, doi: 10.1109/SERVICES.2019.00022.

[4] J. O. Agyemang, J. J. Kponyo, and I. Acquah, "Lightweight Man-In-The-Middle (MITM) Detection and Defense Algorithm for WiFi-Enabled Internet of Things (IoT) Gateways," vol. 7, no. January, pp. 1–6, 2019, doi: 10.12691/iscf-7-1-1.

[5] D. Al Abri, "Detection of MITM attack in LAN environment using payload matching," *Proc. IEEE Int. Conf. Ind. Technol.*, vol. 2015-June, no. June, pp. 1857–1862, 2015, doi: 10.1109/ICIT.2015.7125367.

[6] Y. Yang, K. McLaughlin, T. Littler, S. Sezer, B. Pranggono, and H. F. Wang, "Intrusion Detection System for IEC 60870-5-104 based SCADA networks," *IEEE Power Energy Soc. Gen. Meet.*, no. July, 2013, doi: 10.1109/PESMG.2013.6672100.

[7] X. Zhan, H. Yuan, and X. Wang, "Research on Block Chain Network Intrusion Detection System," *Proc. - 2nd Int. Conf. Comput. Network, Electron. Autom. ICCNEA 2019*, pp. 191–196, 2019, doi: 10.1109/ICCNEA.2019.00045.

[8] L. A. Maglaras and J. Jiang, "Intrusion detection in SCADA systems using machine learning techniques," *Proc. 2014 Sci. Inf. Conf. SAI 2014*, pp. 626–631, 2014, doi: 10.1109/SAI.2014.6918252.

[9] M. A. Teixeira, T. Salman, M. Zolanvari, R. Jain, and M. Samaka, "SCADA System Testbed for Cybersecurity Research Using Machine Learning Approach," no. Ml, pp. 1–15, 2018, doi: 10.3390/fi10080076.

[10] E. Min, J. Long, Q. Liu, J. Cui, and W. Chen, "TR-IDS: Anomaly-Based Intrusion Detection through Text-Convolutional Neural Network and Random Forest," *Secur. Commun. Networks*, vol. 2018, 2018, doi: 10.1155/2018/4943509.

[11] C. T. Lin, S. L. Wu, and M. L. Lee, "Cyber attack and defense on industry control systems," *2017 IEEE Conf. Dependable Secur. Comput.*, pp. 524–526, 2017, doi: 10.1109/DESEC.2017.8073874.

[12] Y. Xu, Y. Yang, T. Li, and Q. Wang, "Review on Cyber Vulnerabilities nf communication Protocols in Industrial Control Systems," 2017.

[13] P. Maynard and K. Mclaughlin, "Towards Understanding Man-In-The-Middle Attacks on IEC 60870-5-104 SCADA Networks," pp. 30–42, 2014.

[14] J. Chromik, A. Remke, B. R. Haverkort, and G. Geist, "A Parser for Deep Packet Inspection of IEC-104: A Practical Solution for Industrial Applications," *Proc. - 49th Annu. IEEE/IFIP Int. Conf. Dependable Syst. Networks - DSN 2019 Ind. Track*, pp. 5–8, 2019, doi: 10.1109/DSN-Industry.2019.00008.

[15] M. Petr, "Description and analysis of IEC 104 Protocol Petr Matoušek," p. 38, 2017.

[16] C. C. Lo, C. C. Huang, and J. Ku, "A cooperative intrusion detection system framework for cloud computing networks," *Proc. Int. Conf. Parallel Process. Work.*, pp. 280–284, 2010, doi: 10.1109/ICPPW.2010.46.

[17] A. Lazarevic, V. Kumar, and J. Srivastava, *Intrusion Detection : A Survey. Managing Cyber Threats*, vol. 5, no. January. 2014.

[18] A. Khraisat, I. Gondal, P. Vamplew, and J. Kamruzzaman, "Survey of intrusion detection systems: techniques, datasets and challenges," *Cybersecurity*, vol. 2, no. 1, 2019, doi: 10.1186/s42400-019-0038-7.

[19] A. Mallik, A. Ahsan, M. M. Z. Shahadat, and J. C. Tsou, "Man-in-the-

middle-attack: Understanding in simple words," *Int. J. Data Netw. Sci.*, vol. 3, no. 2, pp. 77–92, 2019, doi: 10.5267/j.ijdns.2019.1.001.

[20] J. Gómez, C. Gil, N. Padilla, R. Baños, and C. Jiménez, "Design of a Snort-Based Hybrid Intrusion," *Proc. 10th Int. Work. Artif. Neural Networks*, pp. 515–522, 2009.

[21] R. Primartha and B. A. Tama, "Anomaly detection using random forest: A performance revisited," *Proc. 2017 Int. Conf. Data Softw. Eng. ICoDSE 2017*, vol. 2018-Janua, pp. 1–6, 2018, doi: 10.1109/ICODSE.2017.8285847.

[22] A. Gezer, G. Warner, C. Wilson, and P. Shrestha, "A flow-based approach for Trickbot banking trojan detection," *Comput. Secur.*, vol. 84, pp. 179–192, 2019, doi: 10.1016/j.cose.2019.03.013.

[23] N. V. Chawla, K. W. Bowyer, L. O. Hall, and W. P. Kegelmeyer, "SMOTE: Synthetic Minority Over-sampling Technique Nitesh," *Artif. Intelegence Res.*, vol. 30, no. 2, pp. 321–357, 2002, doi: https://doi.org/10.1613/jair.953.

[24] T. Le and S. W. Baik, "A robust framework for self-care problem identification for children with disability," *Symmetry (Basel).*, vol. 11, no. 1, 2019, doi: 10.3390/sym11010089.

[25] P. Maynard, K. McLaughlin, and S. Sezer, "An Open Framework for Deploying Experimental SCADA Testbed Networks," no. 2016, pp. 92–101, 2018, doi: 10.14236/ewic/ics2018.11.

[26] H. Waagsnes, "17 Waagsnes SCADA Intrusion Detection System Test Framework," no. May, 2017.

[27] N. Farnaaz and M. A. Jabbar, "Random Forest Modeling for Network Intrusion Detection System," *Procedia Comput. Sci.*, vol. 89, pp. 213–217, 2016, doi: 10.1016/j.procs.2016.06.047.

[28] S. Sgu, B. Io, S. Sgu, B. Io, and A. Io, "IEC 60870-5-104 Configuration / Interoperability Guide for SICAM SGU 7XV5676 7XV5676-xJLx – SICAM SGU with Binary IO and Analog IO," 2014.