VISUALISASI SERANGAN *MAN IN THE MIDDLE* (MITM) PADA PROTOKOL JARINGAN SCADA(IEC 60870-5-104) MENGGUNAKAN METODE *K-MEANS*

TUGAS AKHIR

DISUSUN OLEH :

Ronnie Radhitya Rafi Al-Kamal

09011381823095

JURUSAN SISTEM KOMPUTER

FAKULTAS ILMU KOMPUTER

UNIVERSITAS SRIWIJAYA

2022

LEMBAR PENGESAHAN

VISUALISASI SERANGAN *MAN IN THE MIDDLE* (MITM) PADA PROTOKOL JARINGAN SCADA(IEC 60870-5-104) MENGGUNAKAN METODE *K-MEANS*

TUGAS AKHIR

Program Studi Sistem Komputer
Jenjang S1

Oleh

Ronnie Radhitya Rafi Al-Kamal

09011381823095

Palembang, Desember 2022

Mengetahui,

Ketua Jurusan Sistem Komputer	Pembimbing Tugas Akhir
Dr. Ir. H. Sukemi, M.T.	**Deris Stiawan, M.T., Ph.D.**
NIP. 196612032006041001	**NIP. 197806172006041002**

HALAMAN PERSETUJUAN

Telah diuji dan lulus pada :

Hari : Jum'at
Tanggal : 11 November 2022

Tim Penguji :

1. **Ketua : Ahmad Zarkasi, S.T., M.T.**
2. **Penguji : Huda Ubaya, S.T., M.T.**
3. **Sekretaris : Tri Wanda Septian, S.Kom., M.Sc.**
4. **Pembimbing : Deris Stiawan, M.T., Ph.D.**

Mengetahui,
Ketua Jurusan Sistem Komputer

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

LEMBAR PERNYATAAN

Yang bertanda tangan dibawah ini:

Nama : Ronnie Radhitya Rafi Al-Kamal

NIM : 09011381823095

Judul : Visualisasi Serangan *Man In The Middle(MITM)* Pada Protokol Jaringan *SCADA(Iec 60870-5-104)* Menggunakan Metode *K-Means*

Hasil Pengecekan Software iThenticate/Turnitin : 16%

Menyatakan bahwa laporan tugas akhir saya merupakan hasil karya sendiri dan bukan hasil penjiplakan / plagiat dari penelitian orang lain. 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, Desember 2022

Penulis,

Ronnie Radhitya Rafi Al-Kamal

NIM. 09011381823095

HALAMAN PERSEMBAHAN

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيم

Skripsi ini penulis dedikasikan kepada kedua orang tua tercinta, Ayahanda dan Ibunda, ketulusanya dari hati atas doa yang tak pernah putus, semangat yang tak ternilai. Serta Untuk Orang-Orang Terdekatku Yang Tersayang, Dan Untuk Almamater Ku Kebanggaanku Program Studi Sistem Komputer Fakultas Ilmu Komputer Universitas Sriwijaya.

Dengan mengucap syukur Alhamdulillah atas rahmat Allah Subhanahu wa Ta'alamyang telah membrikan izin serta ridhonya sehingga penulis mampu memenuhi harapan keluarga besar, rekan seperjuagan, serta civitas akademik agar segera menyelesaikan masa studi untuk mendapatkan gelar sarjana komputer.

"*Keep your eyes on the stars and your feet on the ground*"

"Jaga matamu menghadap ke bintang dan pijakkan kakimu ke tanah"

Desember 2022

KATA PENGANTAR

Assalamu'alaikum Warahmatullahi Wabarakatuh

Puji syukur atas kehadirat Allah SWT karena atas berkat rahmat serta karunia-Nya sehingga penulis dapat menyelesaikan proposal tugas akhir ini yang berjudul **"**Visualisasi Serangan *Man In The Middle(MITM)* Pada Protokol Jaringan *SCADA(Iec 60870-5-104)* Menggunakan Metode *K-Means***"**.

Dalam laporan ini penulis akan membahas tentang virualisasi serangan yang ditemukan pada protokol komunikasi SCADA menggunakan metode *clustering,* untuk menemukan hasil dari pengujian metode yang digunakan. Selain itu, penulis meyakini bahwa dengan adanya laporan ini maka akan dapat bermanfaat kedepanya terhadap kelompok atau orang yang ingin membacanya serta tertarik juga untuk melakukan penelitian terkait *visualisasi serangan Man In The Middle* (MITM).

Sebelumnya, penulis ingin mengucapkan terima kasih kepada beberapa pihak atas pemberian ide dan saran selama penyusunan proposal Tugas Akhir ini. Untuk itu penulis ingin mengucapkan terima kasih kepada :

1. Allah SWT yang telah memberikan rahmat serta karunia-Nya sehingga penulis dapat menyelesaikan Proposal Tugas Akhir ini dengan baik.

2. Orang tua saya tercinta yang telah membesarkan saya hingga saat ini dan tak henti – hentinya dalam memberikan semangat, mengajarkan hal – hal yang baik, dan selalu memberikan doa serta motivasi.

3. Bapak Jaidan Jauhari, S.Pd., M.T., selaku Dekan Fakultas Ilmu Komputer Universitas Sriwijaya.

4. Bapak Dr. Ir. H. Sukemi, M.T., selaku Ketua Jurusan Sistem Komputer Fakultas Ilmu Komputer Universitas Sriwijaya.

5. Bapak Deris Stiawan, M.T., Ph.D. selaku Dosen Pembimbing Tugas Akhir yang telah berkenan meluangkan waktunya guna membimbing, memberikan saran serta memotivasi untuk penulis dalam menyusun Tugas Akhir ini.

6. Bapak Firdaus, M.Kom. selaku Pembimbing Akademik Jurusan Sistem Komputer penulis saat ini.

7. Dan semua pihak yang telah membantu yang penulis tidak bisa sebutkan satu persatu.

Penulis sadar bahwa laporan yang disusun masih sangat jauh dari kata sempurna. Untuk itu penulis meminta kritik dan saran yang membangun sehingga penyusunan akan menjadi lebih baik untuk kedepannya serta menjadi daya tarik penelitian itu sendiri.

Palembang, 14 Januari 2022

Penulis,

Ronnie Radhitya Rafi Al-Kamal
NIM. 09011381823095

VISUALIZATION OF MAN IN THE MIDDLE (MITM) ATTACK ON SCADA NETWORK PROTOCOLS (IEC 60870-5-104) USING K-MEANS METHOD

RONNIE RADHITYA RAFI AL-KAMAL (09011381823095)

Department of Computer Systems, Faculty of Computer Science, Universitas Sriwijaya

Email : radhityaraffi@gmail.com

ABSTRACT

Supervisory Control and Data Acquisition (SCADA) is a system based on software and hardware elements critical to everyday life and the citizens' economy, including oil networks, water treatment plants, and chemical plants. However, SCADA networks often get cyberattacks, for example, "Man in the Middle" (MITM), in which the attacker secretly takes data, transfers it, and even changes correspondence between the two parties where the victim does not realize that the victim is not communicating directly with the destination. In this research, an experiment will be carried out to visualize the Man in the Middle (MITM) attack using the K-Means method. The optimal cluster results were obtained with 2 clusters using the elbow technique. From the visualization results, cluster 1 and cluster 2 have the same pattern and an uneven distribution because a lot of the data has uniformity, so it only forms a particular pattern and does not spread. Then the normal data is more dominant than the attack data.

Keyword : *Supervisory Control and Data Acquisition* (SCADA), *Man In The Middle* (MITM), *K-Means*

VISUALISASI SERANGAN *MAN IN THE MIDDLE* (MITM) PADA PROTOKOL JARINGAN SCADA(IEC 60870-5-104) MENGGUNAKAN METODE *K-MEANS*

RONNIE RADHITYA RAFI AL-KAMAL (09011381823095)

Jurusan Sistem Komputer, Fakultas Ilmu Komputer, Universitas Sriwijaya

Email : radhityaraffi@gmail.com

ABSTRAK

Supervisory Control and Data Acquisition (SCADA) adalah sebuah sistem berbasis perangkat lunak dan beberapa elemen perangkat keras yang sangat penting bagi kehidupan sehari-hari dan bagi ekonomi warga, mencakup jaringan minyak, pengolahan air, dan pabrik kimia. Namun pada jaringan scada kerap kali mendapat serangan siber contohnya Man In The Middle (MITM), serangan ini merupakan sebuah serangan yang mana penyerang mengambil data secara diam-diam, mentransfer bahkan merubah koresponden antar kedua pihak yang mana korban tidak menyadari bahwa korban tidak sedang berkomunikasi langsung ke tujuan. Pada penelitian kali ini akan dilakukan nya percobaan dalam melakukan visualisasi pada serangan Man In The Middle (MITM) menggunakan metode K-Means. Didapatkan hasil cluster yang paling optimal dengan jumlah 2 cluster menggunakan teknik elbow. Dari hasil visualisasi antara cluster 1 dan cluster 2 memiliki pola yang sama memiliki persebaran yang tidak merata, dikarenakan banyak data yang memiliki keseragaman sehingga hanya membentuk pola tertentu dan tidak menyebar. Kemudian untuk data normal lebih dominan dibandingkan data serangan.

Kata Kunci : *Supervisory Control and Data Acquisition* (SCADA), *Man In The Middle* (MITM), *K-Means*

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

BAB I

PENDAHULUAN

1.1 Latar Belakang

Supervisory Control And Data Acquisituion (SCADA), Biasanya digunakan oleh industri yang sangat penting bagi kehidupuan sehari-hari warga dan ekonomi warga, mencakup jaringan pipa minyak, pengolahan air, dan pabrik kimia[1] SCADA bertanggung jawab agar dapat memantau atau dapat mengendalikan dan mengolah pada proses industry dari jarak jauh. Sistem SCADA memiliki perangkat keras, perangkat lunak, dan memiliki jaringan, Arsitektur nya terbentuk oleh *Remote Terminal unite, Intelligent Electronic Device* dan *Programmable Logic Controller* yang saling terhubung. Serangan *cyber* yang berhasil pada system SCADA memungkinkan penyerang dapat mempengaruhi bahkan mengambil alih fungsi.[2]

Man In The Middle (MITM) merupakan sebuah serangan yang memungkinkan penyerang atau pihak ketiga akan diam-diam mengambil, mentransfer bahkan merubah isi dari data antar kedua pihak, dan korban tidak menyadari bahwa korban sedang tidak berkomunikasi langsung ke tujuan yang korban tuju[3]. Penyerang memungkinkan untuk dapat memalsukan informasi untuk mengubah alur komunikasi yang sebenarnya dari pengirim dan penerima, sehingga serangan MITM dapat dilakukan[4]

Pada percobaan yang akan dibuat pada penelitian ini akan berfokus membahas tentang serangan MITM yang terjadi pada protocol *IEC 60870-5-104,* Protokol ini adalah hasil dari gabungan dari IEC 60870-5101 dan dari *Transmission Control Protocola atau Internet Protocol(IP). Application Protocol Data Unit* (APDU) adalah basic fram dari IEC 60870-5-104. Dan

semua itu terbagi menjadi 3 format yang berbeda pada data flow, link monitoring, dan transmisi informasi.

APDU terbagi menjadi 2 yaitu, *Application Protocol Control Information (APCI) dan Application Service Data Unit (ASDU).* APCI adalah sebuah informasi yang terdapat didalam nya ada length dari APDU atau pengirim dan penerima dari sequence numbers dan mempunyai paket length tetap 4 byte. Jika nilai tidak demikian maka ASDU mempunyai variable length untuk dapat menjelaskan apa saja atribut secara rinci *"type Identification atau "Cause of Transmission"*

Pada penelitian sebelumnya [5] Zaman yang modern seperti sekarang, kemajuan teknologi menimbulkan banyak masalah baru yang akan dihadapi, seiring semakin cepatnya perangkat komunikasi maka membuat *SCADA* akan semakin mudah dan rentan terhadap serangan. Terdapat fakta bahwa infrastruktur seperti jaringan listrik, air, pipa minyak dan banyak lagi menjadi target utama serangan *cyber.*

Dalam melakukan deteksi serangan [6] sering kali *Intrusion Detection System* (IDS) digunakan untuk dapat mendeteksi serangan oleh *attacker*. Akan tetapi teknik seperti ini memiliki kelemahan, dimana teknik ini tidak dapat mendeteksi tipe serangan yang baru atau serangan yang tidak ada pada *database*. Maka dari itu [7] untuk dapat mengatasi kelemahan tersebut ialah melakukan visualisasi dengan cara yang sederhana agar dapat memudahkan dalam mengenali dan menyimpulkan pola dari visual. Kemudian Clustering merupakan cara yang paling baik untuk dapat digunakan dalam melakukan analysis dan mendeteksi serangan baru atau serangan yang tidak di ketahui.

Algoritma clustering adalah [8] salah satu dari banyak nya algoritma yang berfungsi untuk melakukan analisis utama dalam data mining. Algoritma clustering dapat mempengaruhi hasil, *clustering* ialah salah satu cara untuk melakukan klasifikasi data yang masih mentah kemudian mencari pola yang tersembunyi di dalam dataset. *K-Means* adalah metode *clustering*

yang sederhana, cepat dan paling banyak digunakan, sehinga membuat aplikasi tersasa lebih praktis dengan metode ini. *K-Means* terbukti sebagai cara yang paling baik dan efektif untuk mendapatkan hasil dari pengelompokan yang baik. Metode ini merupakan algoritma yang mengelompokan *data mining* dan sering dipakai untuk mengelompokan data yang memiliki jumlah besar.

Dari pengkajian diatas, penulis akan melakukan visualisasi serangan *Man In The Middle* menggunakan dataset berbentuk *pcap* yang akan di ekstraksi terlebih dahulu, kemudian dapat dijalankan pada algoritma clustering menggunakan metode *K-Means*

1.2 Rumusan Masalah

Adapun rumusan masalah pada penelitian ini adalah :

1. Bagaimana cara untuk mengelompokan serangan *Man In The Middle* dan data normal?
2. Bagaimana algoritma *K-Means* dalam memvisualkan serangan *Man In The Middle*
3. Bagaimana cara agar dapat membuat grafik data serangan *Man In The Middle* dan data normal

1.3 Batasan Masalah

Batasan masalah yang ada dalam penulisan Tugas Akhir :

1. Metode yang digunakan untuk dapat memvisualisasikan serangan *Man In The Middle* menggunakan *K-Means*
2. Hanya mengenali serangan MITM pada protokol IEC104
3. Data yang di visualkan hanya data normal dan data serangan *Man in The Middle*
4. Menggunakan dataset yang terdapat data normal dan data serangan *Man In The Middle*

5. Tidak membahas tentang sistem pencegahan serangan *Man In The Middle*
6. Pengujian dilakukan secara offline

1.4 Tujuan

Berikut ini adalah tujuan dari penelitian tugas akhir ini, adalah :

1. Bagaimana implementasi dari metode K-Means pada serangan MITM pada protokol IEC 60870-5-104 Scada.
2. Melakukan visualisasi dari serangan MITM pada protokol IEC 60870-5-104 Scada

1.5 Manfaat

Manfaat yang didapatkan dari menyusun Tugas Akhir ini, adalah :

1. Dapat mengetahui bentuk serangan yang terjadi pada protokol IEC 60870-5-104 Scada
2. Mampu memahami pola visualisasi dari serangan MITM yang terjadi pada protokol IEC 60870-5-104 Scada
3. Melakukan implementasi metode K-Means dalam mengetahui pola serangan MITM pada protokol IEC 60870-5-104 Scada
4. Dapat memecahkan masalah keamanan yang terjadi pada protokol komunikasi IEC 60870-5-104 Scada

1.6 Metodologi Penelitian

1. Studi Pustaka

   Pada tahap ini peneliti akan mempelajari lalu mengulas materi materi terkait melalui sumber seperti naskah ilmiah.
2. Pengolahan data

   Pada tahap ini akan membahas bagaimana mengkategorikan data menggunakan metode K-Means

3. Visualisasi

   Pada tahap ini akan dilakukan visualisasi serangan Man In The Middle dan data normal menggunakan metode K-Means

1.7 Sistematika Penulisan

Adapun Sistematika dalam menyusun tugas akhir yang bertujuan untuk memperjelas bagian dari setiap bab, seperti berikut :

BAB I. PENDAHULUAN

Pada bab ini penulis akan menjelaskan tentang tujuan, manfaat, metodologi penelitian serta sistematika penulisan.

BAB II TINJAUAN PUSTAKA

Bab ini akan berisi literature riview, dan itu akan berhubungan dengan konsep penelitian ialah membahas tentang serangan Man In The Middle pada protokol IEC 60870-5-104 Scada

BAB III. METODOLOGI PENELITIAN

Pada bab ini penulis akan menjelaskan mengenai bagaimana penelitian dilakukan secara rinci. Termasuk perician pada bab mengenai penerapan metode K-Means dan konsep penlitian agar tujuan dari target penulis tercapai.

BAB IV. PEMBAHASAN DAN ANALISA

Bab ini akan berisikan penjelasan hasil yang diperoleh dari pengujian yang dilakukan pada tahapan sebelumnya, lalu kemudian data akan di analisa untuk mendapatkan validasi hasil.

BAB V KESIMPULAN DAN SARAN

Pada bab ini akan membahas tentang kesimpulan yang diperoleh dari hasil yang telah dilakukan sebelumnya, serta mendapatkan target tujuan yang ingin di capai, lalu memberikan saran untuk peneliti berikutnya.

DAFTAR PUSTAKA

[1] R. Lopez Perez, F. Adamsky, R. Soua, and T. Engel, "Machine Learning for Reliable Network Attack Detection in SCADA Systems," *Proc. - 17th IEEE Int. Conf. Trust. Secur. Priv. Comput. Commun. 12th IEEE Int. Conf. Big Data Sci. Eng. Trust. 2018*, pp. 633–638, 2018, doi: 10.1109/TrustCom/BigDataSE.2018.00094.

[2] 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.

[3] 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.

[4] Y. Yang, X. Wei, R. Xu, L. Peng, L. Zhang, and L. Ge, "Man-in-the-Middle Attack Detection and Localization Based on Cross-Layer Location Consistency," *IEEE Access*, vol. 8, pp. 103860–103874, 2020, doi: 10.1109/ACCESS.2020.2999455.

[5] M. Zolanvari, M. A. Teixeira, L. Gupta, K. M. Khan, and R. Jain, "Machine Learning-Based Network Vulnerability Analysis of Industrial Internet of Things," *IEEE Internet Things J.*, vol. 6, no. 4, pp. 6822–6834, 2019, doi: 10.1109/JIOT.2019.2912022.

[6] H. Choi, H. Lee, and H. Kim, "Fast detection and visualization of network attacks on parallel coordinates," *Comput. Secur.*, vol. 28, no. 5, pp. 276–288, 2009, doi: 10.1016/j.cose.2008.12.003.

[7] V. No, E. A. Winanto, and A. Heryanto, "Visualisasi Serangan Remote to Local (R2L) Dengan Clustering K-Means," vol. 2, no. 1, pp. 359–362, 2016.

[8] N. Shi, X. Liu, and Y. Guan, "Research on k-means clustering

algorithm: An improved k-means clustering algorithm," *3rd Int. Symp. Intell. Inf. Technol. Secur. Informatics, IITSI 2010*, pp. 63–67, 2010, doi: 10.1109/IITSI.2010.74.

[9] M. A. Teixeira, T. Salman, M. Zolanvari, R. Jain, N. Meskin, and M. Samaka, "SCADA system testbed for cybersecurity research using machine learning approach," *Futur. Internet*, vol. 10, no. 8, 2018, doi: 10.3390/fi10080076.

[10] M. J. Brusco, E. Shireman, and D. Steinley, "A comparison of latent class, K -means, and K -median methods for clustering dichotomous data.," *Psychol. Methods*, vol. 22, no. 3, pp. 563–580, 2017, doi: 10.1037/met0000095.

[11] M. E. Celebi, H. A. Kingravi, and P. A. Vela, "A comparative study of efficient initialization methods for the k-means clustering algorithm," *Expert Syst. Appl.*, vol. 40, no. 1, pp. 200–210, 2013, doi: 10.1016/j.eswa.2012.07.021.

[12] M. A. S. Arifin, D. Stiawan, Susanto, J. Rejito, M. Y. Idris, and R. Budiarto, "Denial of Service Attacks Detection on SCADA Network IEC 60870-5-104 using Machine Learning," *Int. Conf. Electr. Eng. Comput. Sci. Informatics*, vol. 2021-Octob, no. October, pp. 228–232, 2021, doi: 10.23919/EECSI53397.2021.9624255.

[13] Y. Cherdantseva *et al.*, "A review of cyber security risk assessment methods for SCADA systems," *Comput. Secur.*, vol. 56, pp. 1–27, 2016, doi: 10.1016/j.cose.2015.09.009.

[14] D. S. Pidikiti, R. Kalluri, R. K. S. Kumar, and B. S. Bindhumadhava, "SCADA communication protocols: vulnerabilities, attacks and possible mitigations," *CSI Trans. ICT*, vol. 1, no. 2, pp. 135–141, 2013, doi: 10.1007/s40012-013-0013-5.

[15] P. R. Grammatikis, P. Sarigiannidis, A. Sarigiannidis, D. Margounakis,

A. Tsiakalos, and G. Efstathopoulos, “An Anomaly Detection Mechanism for IEC 60870-5-104,” *2020 9th Int. Conf. Mod. Circuits Syst. Technol. MOCAST 2020*, pp. 0–3, 2020, doi: 10.1109/MOCAST49295.2020.9200285.

[16] 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.

[17] K. Mai, X. Qin, N. Ortiz Silva, and A. A. Cardenas, “IEC 60870-5-104 network characterization of a large-scale operational power grid,” *Proc. - 2019 IEEE Symp. Secur. Priv. Work. SPW 2019*, pp. 236–241, 2019, doi: 10.1109/SPW.2019.00051.

[18] W. Tao, X. Chen, and Q. Zhang, “Realization of IEC 60870-5-104 Protocol in DTU,” *Int. J. Comput. Electr. Eng.*, no. January 2010, pp. 815–820, 2010, doi: 10.7763/ijcee.2010.v2.233.

[19] 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.

[20] 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.

[21] J. Gondohanindijo, “Sistem Untuk Mendeteksi Adanya Penyusup (IDS : Intrusion Detection System),” *Semarang*, vol. 2, pp. 46–54, 2011.

[22] M. Tiwari, “Intrusion Detection System,” no. April, pp. 39–57, 2011, doi: 10.1142/9781848164482_0004.

[23] B. MaqboolBeigh, U. Bashir, and M. Chahcoo, “Intrusion Detection and Prevention System: Issues and Challenges,” *Int. J. Comput. Appl.*, vol. 76, no. 17, pp. 26–30, 2013, doi: 10.5120/13340-0701.

[24] M. Egger, G. Eibl, and D. Engel, “Comparison of approaches for intrusion detection in substations using the IEC 60870-5-104 protocol,” *Energy Informatics*, vol. 3, no. Suppl 1, pp. 1–17, 2020, doi: 10.1186/s42162-020-00118-4.

[25] O. Eigner, P. Kreimel, and P. Tavolato, “Detection of man-in-the-middle attacks on industrial control networks,” *Proc. - 2016 Int. Conf. Softw. Secur. Assur. ICSSA 2016*, pp. 64–69, 2017, doi: 10.1109/ICSSA.2016.19.

[26] B. Bhushan, G. Sahoo, and A. K. Rai, “Man-in-the-middle attack in wireless and computer networking - A review,” *Proc. - 2017 3rd Int. Conf. Adv. Comput. Commun. Autom. (Fall), ICACCA 2017*, vol. 2018-Janua, pp. 1–6, 2018, doi: 10.1109/ICACCAF.2017.8344724.

[27] Q. Zhu, J. Pei, X. Liu, and Z. Zhou, “Analyzing commercial aircraft fuel consumption during descent: A case study using an improved K-means clustering algorithm,” *J. Clean. Prod.*, vol. 223, pp. 869–882, 2019, doi: 10.1016/j.jclepro.2019.02.235.

[28] M. Agus Syamsul Arifin, D. Stiawan, Susanto, D. Prasetya, M. Yazid Idris, and R. Budiarto, “Malicious Activity Recognition on SCADA Network IEC 60870-5-104 Protocol,” *IEEE Access*, vol. 104, no. Iec 104, pp. 46–51, 2021, doi: 10.1109/ict-pep53949.2021.9601066.

[29] IEEE Power & Energy Society, C. Qing hua da xue (Beijing, Changsha li gong da xue, C. Zhongguo dian ji gong cheng xue hui (Beijing, and Institute of Electrical and Electronics Engineers, *2019 3rd IEEE Conference on Energy Internet and Energy System Integration: Ubiquitous Energy Network Connecting Everything, EI2 2019*. 2019.

[30] D. Wang, C. Li, S. Wen, S. Nepal, and Y. Xiang, “Man-in-the-Middle Attacks against Machine Learning Classifiers Via Malicious Generative Models,” *IEEE Trans. Dependable Secur. Comput.*, vol. 18, no. 5, pp. 2074–2087, 2021, doi: 10.1109/TDSC.2020.3021008.

[31] H. Qabbaah, G. Sammour, and K. Vanhoof, “Using k-means clustering and data visualization for monetizing logistics data,” *2019 2nd Int. Conf. New Trends Comput. Sci. ICTCS 2019 - Proc.*, pp. 1–6, 2019, doi: 10.1109/ICTCS.2019.8923108.

[32] 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.