Jurnal Pengabdian UNDIKMA:
Jurnal Hasil Pengabdian & Pemberdayaan kepada Masyarakat
https://e-journal.undikma.ac.id/index.php/jpu/index
Email: pengabdian@undikma.ac.id

Vol. 7, No. 2 (Mei 2026)
E-ISSN : 2722-5097
Pg : 796-804

Optimalisasi Keamanan Siber dan AI dalam Akselerasi Transformasi Digital Sektor Industri Sumatera Selatan

Deris Stiawan, Ahmad Heryanto, Nurul Afifah*, Adi Hermansyah, Dian Palupi Rini, Septiani Kusuma Ningruma, Dendi Renaldo Permana
Universitas Sriwijaya, Indonesia.
*Corresponding Author. Email: nurul@unsri.ac.id

Abstract: This community service program aims to strengthen the digital defense system of PT PLN Palembang through the integration of cybersecurity technology and artificial intelligence (AI). As a strategic state-owned enterprise, PT PLN faces the risk of cyberattacks targeting SCADA and ERP systems, which may disrupt national energy resilience. The implementation method of this community service activity was carried out systematically through stages of infrastructure auditing, socialization, intensive training, and direct technology implementation using a participatory-collaborative approach. The instrument utilized in this activity was the SCADA system, which was analyzed through real-time network traffic monitoring using machine learning and deep learning algorithms. The results of this community service activity indicate the successful implementation of a SCADA-based security system capable of providing early detection of zero-day threats, as well as enhancing the capacity of PT PLN's IT personnel in independently managing network security. The impact of this activity is the establishment of a more resilient and secure digital transformation foundation for industries in South Sumatra, while simultaneously reducing dependence on conventional passive security systems.

Article History:
Received: 05-04-2026
Reviewed: 29-04-2026
Accepted: 07-05-2026
Published: 20-05-2026

Key Words:
Cybersecurity; Artificial Intelligence; SCADA; Digital Transformation; PT PLN.

Abstrak: Program pengabdian kepada masyarakat ini bertujuan untuk memperkuat pertahanan digital PT PLN Palembang melalui integrasi teknologi keamanan siber dan kecerdasan buatan (AI). Sebagai BUMN strategis, PT PLN menghadapi risiko serangan siber pada sistem SCADA dan ERP yang dapat mengganggu ketahanan pangan nasional. Metode pelaksanaan pengabdian ini dilakukan secara sistematis melalui tahapan audit infrastruktur, sosialisasi, pelatihan intensif, serta implementasi teknologi secara langsung dengan pendekatan partisipatif-kolaboratif. Instrumen yang digunakan dalam kegiatan ini adalah *SCADA* yang dianalisis melalui pemantauan trafik jaringan secara *real-time* menggunakan algoritma *machine learning* dan *deep learning*. Hasil pengabdian masyarakat ini adalah terimplementasinya perangkat *SCADA* yang mampu memberikan deteksi dini terhadap ancaman *zero-day* serta peningkatan kapasitas SDM IT PT PLN dalam mengelola keamanan jaringan secara mandiri. Dampak dari kegiatan ini adalah terciptanya fondasi transformasi digital yang lebih tangguh dan aman bagi industri di Sumatera Selatan, sekaligus mengurangi ketergantungan pada sistem keamanan pasif konvensional.

Sejarah Artikel:
Diterima: 05-04-2026
Direview: 29-04-2026
Disetujui: 07-05-2026
Diterbitkan: 20-05-2026

Kata Kunci:
Keamanan Siber; Kecerdasan Buatan; SCADA; Transformasi Digital; PT PLN.

How to Cite: Deris Stiawan, Ahmad Heryanto, Nurul Afifah, Adi Hermansyah, Dian Palupi Rini, Septiani Kusuma Ningrum, & Dendi Renaldo Permana. (2026). Optimalisasi Keamanan Siber dan AI dalam Akselerasi Transformasi Digital Sektor Industri Sumatera Selatan . *Jurnal Pengabdian UNDIKMA*, *7*(2), 796-804. https://doi.org/10.33394/jpu.v7i2.20555

https://doi.org/10.33394/jpu.v7i2.20555

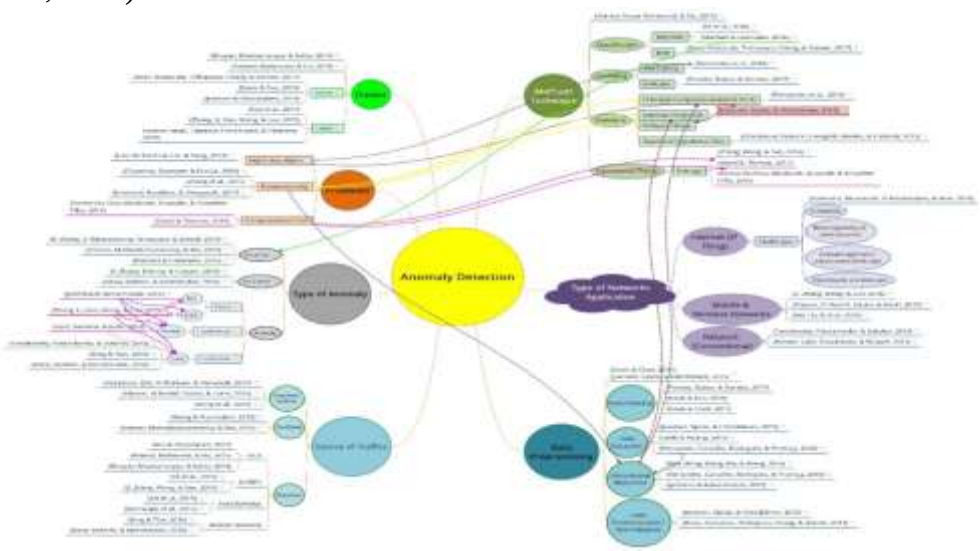
Jurnal Pengabdian UNDIKMA:
Jurnal Hasil Pengabdian & Pemberdayaan kepada Masyarakat
https://e-journal.undikma.ac.id/index.php/jpu/index
Email: pengabdian@undikma.ac.id

Vol. 7, No. 2 (Mei 2026)
E-ISSN : 2722-5097
Pg : 796-804

Pendahuluan

Era Revolusi Industri 4.0 telah membawa perubahan paradigma yang fundamental dalam operasional industri manufaktur dan kimia di Indonesia (Shukla et al., 2023; Taqi et al., 2025). Digitalisasi bukan lagi sekadar pilihan, melainkan kebutuhan strategis untuk mempertahankan efisiensi dan daya saing global (Fadzil et al., 2023; Tharewal et al., 2022). PT PLN Palembang, sebagai perusahaan listrik nasional dan objek vital nasional di Sumatera Selatan, berada di garda terdepan dalam proses transformasi ini. Namun, integrasi sistem teknologi informasi (TI) dengan teknologi operasional (OT) melalui sistem SCADA dan ERP membuka celah kerentanan baru yang bersifat masif (Nazir et al., 2021). Masalah utama yang dihadapi adalah "permukaan serangan" (attack surface) yang meluas, di mana setiap titik konektivitas digital berpotensi menjadi pintu masuk bagi ancaman siber seperti ransomware, phishing, hingga sabotase industri (Akhtar & Gupta, 2021; Altaha & Hong, 2022; Joshi & Shandilya, 2025; Li et al., 2025).

Analisis situasi menunjukkan bahwa sistem keamanan tradisional berbasis *signature based* seringkali gagal mendeteksi ancaman baru atau serangan *zero day* yang polanya belum terdaftar dalam basis data. Serangan sering kali berupa Advanced Persistent Threats (APT) yang mampu bergerak secara lateral di dalam jaringan tanpa terdeteksi. Tanpa sistem berbasis AI, 10% dari anomali berbahaya ini baru teridentifikasi lebih dari 24 jam setelah infiltrasi terjadi, waktu yang lebih dari cukup bagi penyerang untuk melumpuhkan sistem kontrol produksi atau mengeksploitasi data sensitif perusahaan. Tingginya frekuensi dan daya rusak serangan ini menciptakan ancaman eksistensial bagi keberlanjutan operasional perusahaan sebagai objek vital nasional (Panagiotou et al., 2021) (Sommestad et al., 2022). Selain itu, ketergantungan pada proses pemantauan manual menyebabkan respons terhadap anomali jaringan menjadi lambat, yang dalam konteks industri kritikal, keterlambatan hitungan menit dapat menyebabkan kerugian finansial milyaran rupiah hingga gangguan distribusi pupuk nasional. Isu ini diperparah oleh kesenjangan kompetensi sumber daya manusia (SDM) dalam mengadopsi teknologi mutakhir seperti Kecerdasan Buatan (AI) untuk pertahanan digital (Girija et al., 2024).



Gambar 1. Tantangan Transformasi Digital

Jurnal Pengabdian UNDIKMA:
Jurnal Hasil Pengabdian & Pemberdayaan kepada Masyarakat
https://e-journal.undikma.ac.id/index.php/jpu/index
Email: pengabdian@undikma.ac.id

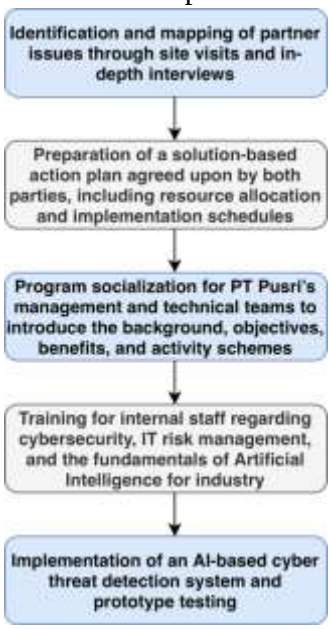
Vol. 7, No. 2 (Mei 2026)
E-ISSN : 2722-5097
Pg : 796-804

Secara teoritis, keamanan siber di sektor industri strategis harus mulai bergeser menuju konsep Cyber Resilience dan Adaptive Security Architecture (Choi et al., 2024). Penggunaan AI, khususnya Machine Learning dan Deep Learning, menawarkan kemampuan untuk mempelajari perilaku normal jaringan dan mendeteksi anomali secara proaktif (Abdelmoumin et al., 2022; Agus Syamsul Arifin et al., 2021, 2024; Arifin et al., 2021; Rafique et al., 2024; Saeed et al., 2023).

Kebijakan pemerintah melalui BSSN dan kementerian terkait juga terus mendorong penguatan infrastruktur informasi kritis. Oleh karena itu, program pengabdian ini sangat mendesak untuk dilaksanakan sebagai jembatan antara kepakaran akademisi di bidang keamanan siber dengan kebutuhan aktual industri. Tujuan dari program pengabdian kepada masyarakat ini adalah untuk mengimplementasikan solusi keamanan siber cerdas berbasis AI yang disebut "SCADA" guna memperkuat postur keamanan digital PT PLN. Selain aspek teknologi, program ini bertujuan meningkatkan kapasitas teknis tenaga IT perusahaan melalui pelatihan intensif dan penyusunan SOP yang mengacu pada standar internasional seperti ISO 27001. Kontribusi yang diharapkan dari program ini tidak hanya terbatas pada proteksi data, tetapi juga pada stabilitas operasional PT PLN dalam mendukung ketahanan pangan nasional melalui kelancaran pengaliran listrik nasional.

Metode Pengabdian

Program pengabdian kepada masyarakat ini dilaksanakan dengan metode kolaboratif-partisipatif yang melibatkan akademisi sebagai penyedia solusi teknologi dan Divisi IT PT PLN Palembang yang terdiri dari tim network engineer, SOC dan administrator jaringan sebagai mitra pelaksana. Kegiatan ini berlangsung selama periode lima bulan (Agustus hingga Desember) dengan fokus lokasi pada Departemen Teknologi Informasi PT PLN. Pendekatan yang digunakan adalah Technology Transfer and Empowerment, di mana tim pengabdi tidak hanya memberikan alat, tetapi juga menularkan pengetahuan (knowledge transfer) agar sistem yang diimplementasikan dapat berkelanjutan secara mandiri.



Gambar 2. Alur Pengabdian

Jurnal Pengabdian UNDIKMA:
Jurnal Hasil Pengabdian & Pemberdayaan kepada Masyarakat
https://e-journal.undikma.ac.id/index.php/jpu/index
Email: pengabdian@undikma.ac.id

Vol. 7, No. 2 (Mei 2026)
E-ISSN : 2722-5097
Pg : 796-804

Tahapan pelaksanaan dimulai dengan Analisis Risiko dan Audit Infrastruktur. Pada tahap ini, tim melakukan identifikasi kerentanan pada topologi jaringan eksisting menggunakan teknik pemindaian pasif dan wawancara mendalam. Data yang diperoleh dari tahap ini menjadi dasar dalam mengonfigurasi model AI pada perangkat SCADA agar sesuai dengan karakteristik trafik jaringan PT PLN. Instrumen utama yang digunakan adalah Network Security Appliance berbasis Small Board Computer (SBC) yang telah diinstalasi dengan engine pendeteksi anomali berbasis Machine Learning. Tahap kedua adalah Workshop dan Pelatihan Interaktif. Metode pelatihan dilakukan melalui simulasi serangan siber (Cyber Drill) dan praktik langsung konfigurasi perangkat. Materi pelatihan mencakup dasar-dasar Network Security, pengenalan algoritma Deep Learning untuk deteksi intrusi, hingga manajemen insiden. Tahap ketiga adalah Implementasi dan Pendampingan Teknis. Perangkat SCADA dipasang pada titik-titik strategis jaringan untuk memantau trafik secara real-time. Evaluasi akhir program dilakukan melalui observasi performa sistem dalam mendeteksi trafik berbahaya dan dokumentasi teknis yang disusun bersama antara tim pengabdi dan mitra. Dengan metode ini, program diharapkan dapat memberikan dampak yang terukur baik dari sisi teknis maupun peningkatan kapabilitas organisasi.

Tabel 1. Rancangan evaluasi kegiatan PKM Skema Terintegrasi

No	Kriteria	Indikator Pencapaian
1	Kesiapan komponen dalam Perancangan dan implementasi sistem SCADA	Semua komponen pelatihan tersedia dan mudah di dapatkan
2	Perancangan SCADA	Berjalan dengan baik tanpa kendala
3	Perancangan program sistem SCADA	Berjalan dengan baik tanpa kendala
4	Integrasi sistem SCADA	Tidak ada kesulitan bagi peserta dalam mengintegrasikan sistem ini ke dalam SCADA
5	feedback untuk evaluasi kegiatan pelatihan.	Respon positif

Data yang diperoleh melalui wawancara, observasi langsung selama proses integrasi sistem, serta *feedback* dari mitra dianalisis menggunakan teknik deskriptif kualitatif. Pendekatan ini difokuskan untuk mengevaluasi dimensi intervensi yang bersifat non-numerik, seperti tingkat sinkronisasi antara SOP keamanan siber yang baru disusun dengan budaya kerja organisasi di PT PLN. Selain itu, teknik ini digunakan untuk membedah pengalaman pengguna (*user experience*) terhadap antarmuka AI serta mengidentifikasi secara mendalam berbagai kendala teknis yang muncul di lapangan selama fase instalasi. Dengan analisis deskriptif kualitatif, tim pengabdi dapat menyusun rekomendasi perbaikan yang lebih kontekstual dan aplikatif bagi keberlanjutan teknologi di lingkungan industri mitra.

Jurnal Pengabdian UNDIKMA:
Jurnal Hasil Pengabdian & Pemberdayaan kepada Masyarakat
https://e-journal.undikma.ac.id/index.php/jpu/index
Email: pengabdian@undikma.ac.id

Vol. 7, No. 2 (Mei 2026)
E-ISSN : 2722-5097
Pg : 796-804

Hasil Pengabdian dan Pembahasan

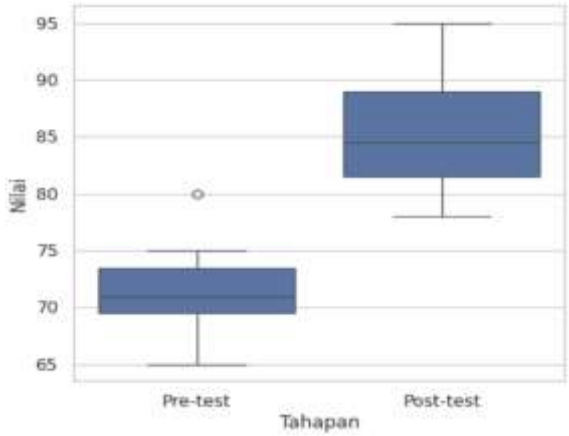
Hasil utama dari kegiatan ini adalah keberhasilan instalasi dan integrasi perangkat SCADA sebagai lapisan pertahanan tambahan dalam arsitektur keamanan PT PLN. Berdasarkan uji coba lapangan, sistem ini mampu melakukan pemindaian trafik secara kontinu tanpa menyebabkan latency yang signifikan pada jaringan operasional. Inovasi penggunaan AI dalam perangkat ini terbukti mampu mengidentifikasi pola trafik yang mencurigakan yang sebelumnya luput dari pemantauan firewall standar. Perangkat ini tidak hanya berfungsi sebagai IDS (Intrusion Detection System), tetapi juga mampu memberikan rekomendasi blokir otomatis pada fungsi IPS (Intrusion Prevention System), yang secara drastis mempercepat Response Time terhadap potensi serangan.

Gambar 3. SCADA

Dari sisi pengembangan kapasitas SDM, terjadi peningkatan signifikan pada pengetahuan teknis peserta pelatihan. Para staf IT kini memiliki pemahaman yang lebih dalam mengenai cara kerja algoritma Machine Learning dalam mengklasifikasikan trafik normal dan anomali. Diskusi selama pelatihan mengungkap bahwa tantangan terbesar selama ini adalah rasa kurang percaya diri dalam mengelola AI karena dianggap terlalu kompleks. Namun, melalui pendekatan simulasi praktis, hambatan psikologis tersebut berhasil diatasi. Peserta kini mampu mengoperasikan dashboard SCADA untuk melakukan investigasi mandiri terhadap setiap peringatan keamanan yang muncul. Diskusi kritis terhadap program ini menyoroti pentingnya sinkronisasi antara teknologi canggih dengan kebijakan organisasi. Implementasi SCADA harus didukung oleh SOP yang kuat agar setiap notifikasi serangan ditindaklanjuti dengan prosedur yang baku. Oleh karena itu, penyusunan draf kebijakan keamanan siber dalam program ini menjadi pencapaian yang setara pentingnya dengan perangkat keras itu sendiri. Tantangan yang ditemukan selama implementasi adalah adanya protokol komunikasi industri lama yang menghasilkan pola trafik tidak beraturan sehingga sempat memicu false positive pada AI. Tim kemudian melakukan fine-tuning atau penyesuaian parameter algoritma untuk mengenali protokol tersebut sebagai trafik legal, yang menunjukkan bahwa AI keamanan siber memerlukan proses pembelajaran yang spesifik untuk setiap lingkungan industri.

Jurnal Pengabdian UNDIKMA:
Jurnal Hasil Pengabdian & Pemberdayaan kepada Masyarakat
https://e-journal.undikma.ac.id/index.php/jpu/index
Email: pengabdian@undikma.ac.id

Vol. 7, No. 2 (Mei 2026)
E-ISSN : 2722-5097
Pg : 796-804



Gambar 4. Hasil Evaluasi

Tabel 2. Capaian Hasil Pengabdian Masyarakat

No	Kriteria Evaluasi	Indikator Pencapaian	Status Capaian	Keterangan
1	Kesiapan Komponen	Ketersediaan perangkat keras (SBC), modul pelatihan, dan akses logistik dalam perancangan sistem SCADA.	100%	Semua komponen tersedia lengkap dan mudah didapatkan sebelum kegiatan dimulai.
2	Perancangan SCADA	Desain arsitektur perangkat keras dan pemilihan spesifikasi sistem keamanan.	Berhasil	Perancangan fisik alat selesai sesuai spesifikasi industrial-grade tanpa kendala teknis.
3	Perancangan Program	Pengembangan algoritma AI (Machine Learning) dan antarmuka dashboard pemantauan.	Berhasil	Kode program berjalan stabil dan mampu mengklasifikasikan trafik jaringan secara akurat.
4	Integrasi Sistem	Proses pemasangan dan sinkronisasi sistem SCADA ke dalam jaringan eksisting mitra.	Lancar	Peserta dan tim IT mitra mampu mengintegrasikan sistem ke arsitektur jaringan tanpa gangguan operasional.
5	Feedback Pelatihan	Evaluasi respon, tingkat kepuasan, dan pemahaman peserta terhadap materi yang diberikan.	Sangat Positif	Peserta memberikan apresiasi tinggi; nilai post-test menunjukkan peningkatan kapasitas SDM yang signifikan.

Secara keseluruhan, kegiatan ini membuktikan bahwa sinergi antara akademisi dan industri sangat efektif dalam mengakselerasi transformasi digital yang aman (Taqi et al., 2025) (Rahman et al., 2025). PT PLN kini memiliki fondasi keamanan yang lebih tangguh dan adaptif, yang sangat krusial bagi keberlangsungan operasionalnya sebagai penyokong

Jurnal Pengabdian UNDIKMA:
Jurnal Hasil Pengabdian & Pemberdayaan kepada Masyarakat
https://e-journal.undikma.ac.id/index.php/jpu/index
Email: pengabdian@undikma.ac.id

Vol. 7, No. 2 (Mei 2026)
E-ISSN : 2722-5097
Pg : 796-804

ketahanan pangan nasional. Keberhasilan ini menegaskan bahwa inovasi teknologi yang disertai dengan edukasi dan standarisasi prosedur adalah kunci utama dalam menghadapi tantangan di era Revolusi Industri 4.0.

Kesimpulannya, integrasi AI ke dalam keamanan siber industri di Sumatera Selatan, khususnya di PT PLN, telah memberikan dampak nyata pada ketangguhan digital perusahaan. Hasil ini sejalan dengan teori Defense in Depth, di mana keamanan tidak bisa mengandalkan satu alat saja, melainkan harus berupa lapisan-lapisan yang saling melengkapi antara teknologi (SCADA) dan manusia (SDM Terlatih).

Kesimpulan

Program pengabdian kepada masyarakat ini telah berhasil mencapai seluruh target yang ditetapkan, dengan hasil utama berupa penguatan infrastruktur digital PT PLN Palembang melalui penerapan teknologi keamanan siber berbasis AI. Implementasi perangkat SCADA telah memberikan solusi nyata atas kerentanan terhadap serangan siber yang kian kompleks, sekaligus mempercepat kemampuan deteksi dini perusahaan. Selain aspek teknis, program ini telah meningkatkan kapasitas sumber daya manusia di divisi IT secara signifikan, memberikan mereka keterampilan praktis dalam mengelola dan memanfaatkan kecerdasan buatan untuk pertahanan jaringan.

Saran

Berdasarkan hasil pelaksanaan program, terdapat beberapa rekomendasi strategis. Pertama, bagi PT PLN, disarankan untuk terus melakukan pembaruan berkala pada basis data model AI di dalam sistem SCADA agar tetap relevan dengan tren serangan siber terbaru. Perusahaan juga perlu mendorong sertifikasi internasional bagi staf IT guna mempertahankan standar kompetensi yang telah dibangun selama program ini. Kedua, bagi Pemerintah Daerah dan Instansi Terkait, program semacam ini perlu direplikasi pada industri strategis lainnya di Sumatera Selatan untuk menciptakan ekosistem digital wilayah yang aman secara kolektif. Ketiga, bagi Akademisi dan Praktisi selanjutnya, disarankan untuk mengeksplorasi penggunaan Federated Learning agar AI dapat belajar dari berbagai titik serangan tanpa harus membagikan data sensitif antar perusahaan. Terakhir, aspek keberlanjutan program harus dijamin melalui komunikasi rutin antara tim pengabdi dan mitra untuk memastikan teknologi yang diberikan tetap berfungsi optimal dalam jangka panjang.

Ucapan Terima Kasih

Penulis menyampaikan ucapan terima kasih kepada Lembaga Penelitian dan Pengabdian kepada Masyarakat (LPPM) Universitas Sriwijaya atas dukungan pendanaan dan fasilitas yang diberikan dalam pelaksanaan kegiatan pengabdian ini. Penghargaan ini secara khusus didasarkan pada Surat Keputusan Nomor: 0014/UN9/SK.LPPM.PM/2025 tertanggal 17 September 2025. Dukungan tersebut telah menjadi faktor penting dalam keberhasilan implementasi teknologi keamanan siber dan AI bagi mitra industri.

Vol. 7, No. 2 (Mei 2026)
E-ISSN : 2722-5097
Pg : 796-804

Daftar Pustaka

Abdelmoumin, G., Rawat, D. B., & Rahman, A. (2022). On the Performance of Machine Learning Models for Anomaly-Based Intelligent Intrusion Detection Systems for the Internet of Things. *IEEE Internet of Things Journal*, *9*(6), 4280–4290. https://doi.org/10.1109/JIOT.2021.3103829

Agus Syamsul Arifin, M., Stiawan, D., Suprapto, B. Y., Susanto, Salim, T., Idris, M. Y., Shenify, M., & Budiarto, R. (2024). A Novel Dataset for Experimentation with Intrusion Detection Systems in SCADA Networks using IEC 60870-5-104 Standard. *IEEE Access*, *12*, 170553–170569. https://doi.org/10.1109/ACCESS.2024.3473895

Agus Syamsul Arifin, M., Stiawan, D., Susanto, Prasetya, D., Idris, M. Y., & Budiarto, R. (2021). Malicious Activity Recognition on SCADA Network IEC 60870-5-104 Protocol. *ICT-PEP 2021 - International Conference on Technology and Policy in Energy and Electric Power: Emerging Energy Sustainability, Smart Grid, and Microgrid Technologies for Future Power System, Proceedings*, 46–51. https://doi.org/10.1109/ICT-PEP53949.2021.9601066

Akhtar, T., & Gupta, B. B. (2021). Analysing smart power grid against different cyber attacks on SCADA system. *International Journal of Innovative …*. https://doi.org/10.1504/IJICA.2021.116656

Altaha, M., & Hong, S. (2022). Anomaly Detection for SCADA System Security Based on Unsupervised Learning and Function Codes Analysis in the DNP3 Protocol. *Electronics (Switzerland)*, *11*(14). https://doi.org/10.3390/electronics11142184

Arifin, M. A. S., Susanto, 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), 874–883. https://doi.org/10.11591/ijeecs.v22.i2.pp874-883

Choi, W., Pandey, S., & Kim, J. (2024). Detecting Cybersecurity Threats for Industrial Control Systems Using Machine Learning. *IEEE Access*, *12*, 153550–153563. https://doi.org/10.1109/access.2024.3478830

Fadzil, L. M., Manickam, S., & Al-Shareeda, M. A. (2023). A Review of An Emerging Cyber Kill Chain Threat Model. *2nd International Conference on Advanced Computer Applications, ACA 2023*, 157–161. https://doi.org/10.1109/ACA57612.2023.10346959

Girija, R., Abiram, G., Durgadevi, P., & Savita. (2024). Case Study: Artificial Intelligence and Machine Learning in Cybersecurity. *Artificial Intelligence for Cyber Defense and Smart Policing*, 172–176. https://doi.org/10.1201/9781003251781-12

Joshi, I. P., & Shandilya, V. K. (2025). Anomaly Detection and Threat Intelligence With Machine Learning. *Exploiting Machine Learning for Robust Security*, 69–98. https://doi.org/10.4018/979-8-3693-7758-1.ch004

Li, D., Tang, J., Wu, S., Zheng, Z., & Ng, S.-K. (2025). Cyber-Attack Detection and Localization for SCADA system of CPSs. *2025 IEEE/ACM Second International Conference on AI Foundation Models and Software Engineering (Forge)*, 269–279. https://doi.org/10.1109/forge66646.2025.00038

Nazir, S., Patel, S., & Patel, D. (2021). Autoencoder Based Anomaly Detection for SCADA Networks. *International Journal of Artificial Intelligence and Machine Learning*,

Vol. 7, No. 2 (Mei 2026)
E-ISSN : 2722-5097
Pg : 796-804

11(2), 83–99. https://doi.org/10.4018/ijaiml.20210701.oa6

Panagiotou, P., Mengidis, N., Tsikrika, T., Vrochidis, S., & Kompatsiaris, I. (2021). Host-based Intrusion Detection Using Signature-based and AI-driven Anomaly Detection Methods. *Information & Security: An International Journal*, *50*, 37–48. https://doi.org/10.11610/isij.5016

Rafique, S. H., Abdallah, A., Musa, N. S., & Murugan, T. (2024). Machine Learning and Deep Learning Techniques for Internet of Things Network Anomaly Detection—Current Research Trends. *Sensors*, *24*(6). https://doi.org/10.3390/s24061968

Rahman, M. S., Hossain, M. S., Rahman, M. K., Islam, M. R., Sumon, M. F. I., Siam, M. A., & Debnath, P. (2025). Enhancing Supply Chain Transparency with Blockchain: A Data-Driven Analysis of Distributed Ledger Applications. *Journal of Business and Management Studies*, *7*(3), 59–77. https://doi.org/10.32996/jbms.2025.7.3.7

Saeed, M. M., Saeed, R. A., Abdelhaq, M., Alsaqour, R., Hasan, M. K., & Mokhtar, R. A. (2023). Anomaly Detection in 6G Networks Using Machine Learning Methods. *Electronics (Switzerland)*, *12*(15). https://doi.org/10.3390/electronics12153300

Shukla, A. K., Srivastav, S., Kumar, S., & Muhuri, P. K. (2023). UInDeSI4.0: An efficient Unsupervised Intrusion Detection System for network traffic flow in Industry 4.0 ecosystem. *Engineering Applications of Artificial Intelligence*, *120*, 105848.

Sommestad, T., Holm, H., & Steinvall, D. (2022). Variables influencing the effectiveness of signature-based network intrusion detection systems. *Information Security Journal*, *31*(6), 711–728. https://doi.org/10.1080/19393555.2021.1975853

Taqi, H. M. M., Nayeem, I., Bari, A. B. M. M., Anam, M. Z., & Ali, S. M. (2025). Addressing challenges to cloud manufacturing in industry 4.0 environment using an integrated approach: Implications for sustainability. *Green Technologies and Sustainability*, *3*(3). https://doi.org/10.1016/j.grets.2024.100166

Tharewal, S., Ashfaque, M. W., Banu, S. S., Uma, P., Hassen, S. M., & Shabaz, M. (2022). Intrusion Detection System for Industrial Internet of Things Based on Deep Reinforcement Learning. *Wireless Communications and Mobile Computing*, *2022*. https://doi.org/10.1155/2022/9023719

