JURNAL FASILKOM
Volume 16 No. 1 | April 2026: 134-149

P-ISSN : 2089-3353
E-ISSN : 2808-9162

H-ASICS: Desain *Intrusion Detection System* Adaptif Berbasis *Hybrid Deep Learning* untuk Infrastruktur Kritis

Andri Yudha Pratama[1]*, Erik IH Ujianto[2], Rianto[3]
[1,2,3]Magister Teknologi Informasi, Fakultas Sains dan Teknologi, Universitas Teknologi Yogyakarta
[1]Badan Kepegawaian Daerah Daerah Istimewa Yogyakarta
[1]pratama.andriyudha@gmail.com*, [2]erik.iman@uty.ac.id, [3]rianto@uty.ac.id

Abstract

The digital transformation of critical infrastructure, particularly Smart Grid and SCADA systems, has exposed new vulnerabilities to complex cyber-attacks such as False Data Injection (FDI), necessitating proactive defense mechanisms that transcend conventional approaches. Through a Systematic Literature Review (SLR) of 51 state-of-the-art studies (2022–2026), this research confirms a paradigm shift from static Deep Learning models toward adaptive, transparent, and decentralized detection ecosystems. Addressing the critical trade-off between high accuracy and operational latency, this study proposes the conceptual framework of H-ASICS (Hybrid Adaptive System for Infrastructure Critical Security). Based on a closed-loop MAPE-K architecture, H-ASICS dynamically selects the most optimal detection algorithms switching between Hybrid CNN-LSTM for complex spatial-temporal patterns and LightGBM for edge computing efficiency. Addressing the critical trade-off between high accuracy and operational latency, this study proposes the conceptual framework of H-ASICS (Hybrid Adaptive System for Infrastructure Critical Security). Based on a closed-loop MAPE-K architecture, H-ASICS dynamically selects the most optimal detection algorithms switching between Hybrid CNN-LSTM for complex spatial-temporal patterns (yielding up to 99.81% detection accuracy) and LightGBM for edge computing efficiency (reducing operational latency to under 10 ms). The superiority of H-ASICS is further reinforced by the integration of Explainable AI (XAI) and blockchain technology to guarantee the transparency of mitigation decisions and the immutability of cyber forensic data. This proposed architecture provides a strategic roadmap for next-generation security systems that are not only accurate and resilient but also highly accountable.

Keywords: artificial intelligence, intrusion detection system, critical infrastructure, smart grid, SCADA

Abstrak

Transformasi digital pada infrastruktur kritis, khususnya sistem *Smart Grid* dan SCADA, telah mengekspos kerentanan baru terhadap serangan siber kompleks seperti *False Data Injection* (FDI), sehingga menuntut mekanisme pertahanan proaktif yang melampaui pendekatan konvensional. Melalui *Systematic Literature Review* (SLR) terhadap 51 literatur mutakhir (2022–2026), studi ini mengonfirmasi pergeseran paradigma dari model *Deep Learning* statis menuju ekosistem deteksi yang adaptif, transparan, dan terdesentralisasi. Menjawab kesenjangan krusial antara akurasi tinggi dan latensi operasional, penelitian ini mengusulkan kerangka kerja konseptual H-ASICS (*Hybrid Adaptive System for Infrastructure Critical Security*). Berbasis arsitektur siklus tertutup MAPE-K, H-ASICS secara dinamis memilih algoritma deteksi yang paling optimal beralih antara *Hybrid* CNN-LSTM untuk pola spasial-temporal yang rumit dan LightGBM untuk efisiensi pada *edge computing*. Menjawab kesenjangan krusial antara akurasi tinggi dan latensi operasional, penelitian ini mengusulkan kerangka kerja konseptual H-ASICS (*Hybrid Adaptive System for Infrastructure Critical Security*). Berbasis arsitektur siklus tertutup MAPE-K, H-ASICS secara dinamis memilih algoritma deteksi yang paling optimal beralih antara *Hybrid* CNN-LSTM untuk mengakomodasi pola spasial-temporal yang rumit (dengan potensi akurasi deteksi mencapai 99,81%) dan *Light*GBM untuk efisiensi pada *edge computing* (guna menekan latensi operasional hingga di bawah 10 ms). Keunggulan H-ASICS semakin diperkuat dengan integrasi *Explainable AI* (XAI) dan teknologi *blockchain* guna menjamin transparansi keputusan mitigasi serta imutabilitas data forensik siber. Rancang bangun ini memberikan peta jalan strategis untuk sistem keamanan masa depan yang tidak hanya akurat dan tangguh, tetapi juga akuntabel.

Kata kunci: *artificial intelligence*, *intrusion detection system*, infrastruktur kritis, *smart grid*, SCADA

1. Pendahuluan

Digitalisasi di sektor energi menjadi komponen penting dalam transformasi digital nasional yang didorong oleh pemerintah. Beberapa bentuk penerapannya di Indonesia mencakup pengembangan *smart grid*, pemanfaatan *Internet of Things* (IoT), serta layanan pelanggan berbasis digital [1]. Teknologi yang dikenal sebagai *Internet of Things* (IoT) menggabungkan berbagai perangkat melalui koneksi internet, yang memungkinkan pertukaran data, pemantauan, dan pengendalian sistem secara otomatis [2]. *Smart grid* merupakan sistem ketenagalistrikan modern yang bersifat cerdas dan terintegrasi, yang menggabungkan berbagai teknologi mutakhir, seperti sensor, *smart* meter, sistem siber-fisik (*Cyber-Physical Systems*–CPS), perangkat *Internet of Things* (IoT), serta

P-ISSN : 2089-3353
E-ISSN : 2808-9162

mekanisme pengendalian berbasis jaringan komunikasi [3].

Transformasi digital yang berlangsung pada sektor infrastruktur kritis, mencakup bidang energi, sistem kelistrikan berbasis *smart grid*, serta sistem kendali industri *Supervisory Control and Data Acquisition* (SCADA), telah mendorong terjadinya konvergensi yang semakin intensif antara Teknologi Operasional (*Operational Technology*/OT) dan Teknologi Informasi (*Information Technology*/IT) [4]. Listrik telah menjadi elemen esensial dalam kehidupan modern, berperan sebagai sumber energi utama yang mendukung berbagai sektor, mulai dari rumah tangga, industri, hingga transportasi [5].

Dalam konteks paradigma Industri 4.0, infrastruktur tersebut berkembang menjadi *Cyber-Physical Systems* (CPS) yang terintegrasi dan saling terhubung guna meningkatkan efisiensi serta efektivitas operasional. Namun, tingkat integrasi dan konektivitas yang tinggi tersebut secara simultan memperluas permukaan serangan (*attack surface*), sehingga meningkatkan risiko paparan terhadap berbagai bentuk ancaman siber [6].

Supervisory Control and Data Acquisition (SCADA) merupakan sistem kontrol industri yang berfungsi untuk memantau dan mengendalikan proses operasional pada berbagai sektor kritis, seperti energi, air, transportasi, dan sektor strategis lainnya. Seiring dengan perkembangan dan adopsinya yang semakin luas dari waktu ke waktu, sistem SCADA menjadi semakin terekspos terhadap berbagai kerentanan, khususnya yang disebabkan oleh meningkatnya ancaman siber [7].

Peningkatan ancaman siber yang kompleks pada sistem SCADA menjadi isu krusial di tengah transisi menuju arsitektur jaringan yang lebih terbuka dan terhubung secara eksternal. Kebutuhan aksesibilitas ini berimplikasi pada terekspos nya celah keamanan sistem. Urgensi penerapan *Intrusion Detection System* (IDS) sebagai mekanisme peringatan dini ditekankan untuk memitigasi berbagai ancaman keamanan pada jaringan SCADA [8].

Laporan *Global Cybersecurity Index* tahun 2024 yang dirilis oleh *International Telecommunication Union* (ITU) menunjukkan bahwa meningkatnya jumlah populasi yang terhubung ke internet yang telah mencapai sekitar 5,4 miliar pengguna berimplikasi pada eskalasi risiko serangan siber terhadap layanan esensial pemerintah serta berbagai sektor infrastruktur kritis [9].

Pada tingkat nasional, Badan Siber dan Sandi Negara (BSSN) melaporkan terjadinya lonjakan signifikan pada aktivitas anomali trafik jaringan. Sepanjang tahun 2023, BSSN mencatat puncak anomali yang mencapai lebih dari 78.464.385 insiden hanya pada bulan Agustus, yang menunjukkan bahwa Indonesia berada pada posisi strategis sebagai salah satu sumber sekaligus target utama anomali trafik siber di tingkat global [10].

Meningkatnya aktivitas online telah menyebabkan kenaikan serangan siber di Indonesia sebagaimana dilaporkan oleh BSSN, hal ini memperlihatkan pentingnya pengembangan sistem keamanan yang lebih efektif untuk menjaga keamanan infrastruktur kritis dari berbagai bentuk ancaman siber [11]. Melonjaknya intensitas serangan siber menuntut penguatan mekanisme keamanan jaringan untuk mengatasi potensi serangan yang belum pernah muncul maupun yang tidak diprediksi sebelumnya. Sistem IDS dapat dimanfaatkan sebagai lapisan pertahanan pertama dalam mendeteksi ancaman dan serangan siber [12]. Serangan siber modern seperti *False Data Injection* (FDI), *Distributed Denial of Service* (DDoS), dan serangan *ransomware* yang menargetkan sistem kontrol industri (ICS) telah menunjukkan bahwa pendekatan pertahanan tradisional seperti *firewall* dan IDS berbasis tanda tangan (*signature-based*) tidak lagi mampu memberikan perlindungan yang memadai terhadap kompleksitas dan dinamika ancaman saat ini [13].

Keamanan siber global menunjukkan pergeseran signifikan menuju pendekatan berbasis anomali (*anomaly-based*), yang mengintegrasikan pemanfaatan kecerdasan buatan (*Artificial Intelligence*/AI). Hasil tinjauan literatur pada rentang tahun 2024–2025 mengindikasikan bahwa algoritma *Deep Learning* (DL), khususnya *Convolutional Neural Networks* (CNN) dan *Long Short-Term Memory* (LSTM), memiliki kemampuan yang unggul dalam mengekstraksi fitur kompleks dari lalu lintas jaringan industri secara waktu nyata. Lebih lanjut, sebuah studi terkini melaporkan bahwa arsitektur LSTM mampu mencapai tingkat akurasi hingga 99,81% dalam mendeteksi serangan pada sistem smart grid, sehingga memperkuat relevansinya sebagai pendekatan yang efektif untuk meningkatkan keamanan infrastruktur kritis [14].

Tinjauan pustaka sebelumnya telah mengeksplorasi penerapan algoritma Deep Learning secara luas pada sistem SCADA. Sebagai contoh, studi komprehensif yang telah memetakan implementasi algoritma dasar seperti CNN, RNN, dan DBN dalam sistem deteksi intrusi [15]. Namun, ulasan tersebut memiliki keterbatasan karena berfokus pada literatur periode 2015–2022 , di mana mayoritas model masih dievaluasi menggunakan *dataset* konvensional seperti KDD99 untuk mendeteksi vektor serangan dasar (seperti DoS atau Probe). Lebih lanjut, studi tersebut hanya bersifat deskriptif dan sekadar merekomendasikan perlunya teknik hibrida atau integrasi blockchain di masa depan, tanpa menawarkan usulan kerangka kerja yang konkret.

Penelitian ini hadir untuk mengisi kesenjangan tersebut dengan mensintesis literatur yang jauh lebih mutakhir (2022–2026), yang berfokus pada ancaman siber-fisik kompleks pada *Smart Grid*, seperti *False Data*

P-ISSN : 2089-3353
E-ISSN : 2808-9162

Injection (FDI). Berbeda dengan review paper sebelumnya yang berhenti pada tahap evaluasi metode eksisting, *Systematic Literature Review* (SLR) ini bertindak sebagai landasan analitis untuk merumuskan sebuah kebaruan (*novelty*) berupa rancang bangun arsitektur konseptual mandiri, yakni H-ASICS (*Hybrid Adaptive System for Infrastructure Critical Security*). Pendekatan ini mengonversi rekomendasi teoretis dari studi terdahulu menjadi sebuah arsitektur pragmatis berbasis MAPE-K yang secara adaptif mengintegrasikan *Hybrid* CNN-LSTM, algoritma *edge-efficient* (LightGBM), *Explainable AI* (XAI), dan imutabilitas *blockchain*.

Penelitian ini didasarkan pada *systematic literature review* (SLR) yang diproyeksikan untuk memberikan kontribusi signifikansi dalam keamanan siber. Fokus utamanya adalah menciptakan arsitektur pertahanan yang adaptif, sebagai respons strategis terhadap eskalasi ancaman siber dalam ekosistem transformasi digital saat ini. Berdasarkan kesenjangan yang telah diidentifikasi serta pesatnya perkembangan teknologi, penelitian ini mengusulkan rancang bangun IDS berbasis AI. Sistem ini dikonfigurasi untuk memberikan performa yang andal dalam mengamankan ekosistem *Smart Grid*, SCADA, dan Industri 4.0 dari ancaman siber yang kompleks.

Oleh karena itu, penelitian ini bertujuan utama untuk melaksanakan *Systematic Literature Review* (SLR) terhadap berbagai studi yang mengkaji penerapan *Artificial Intelligence* pada *Intrusion Detection System* (IDS) di lingkungan *Smart Grid* dan SCADA. Melalui proses pemetaan, sintesis, dan analisis sistematis terhadap penelitian-penelitian yang relevan, penelitian ini diharapkan mampu memberikan pemahaman yang komprehensif mengenai aspek keamanan pada sistem *Smart Grid* dan SCADA, sekaligus memperkuat evaluasi terhadap efektivitas serta kecukupan standar keamanan yang ada.

2. Metode Penelitian

Metodologi *Systematic Literature Review* (SLR) digunakan dalam penelitian ini untuk menemukan, mengkaji, dan mengevaluasi hasil penelitian secara keseluruhan untuk menjawab pertanyaan penelitian. Merumuskan pertanyaan penelitian, melakukan penelitian literatur, menentukan standar inklusi dan eksklusi, memilih literatur, menampilkan data, menyiapkan data, dan menarik kesimpulan dari penelitian ini adalah bagian dari prosesnya. Ruang lingkup literatur menggunakan pencarian ilmiah dari dua *database* yaitu *Google Scholar* dan *ScienceDirect*.

Pertanyaan penelitian utama akan dijawab dengan mempertimbangkan pertanyaan penelitian sekunder berikut:

1) Bagaimana perbandingan kinerja teknik *Hybrid Deep Learning* (seperti CNN-LSTM atau *Autoencoder*-GRU) dibandingkan dengan algoritma *Machine Learning* tunggal dalam mendeteksi serangan siber yang memiliki ketergantungan waktu (temporal *dependencies*) pada jaringan *Smart Grid* dan SCADA?

2) Metode *Explainable AI* (XAI) manakah yang paling efektif diterapkan untuk menginterpretasikan keputusan model IDS, dan bagaimana dampaknya terhadap kepercayaan operator dalam mitigasi insiden?

3) Jenis serangan siber apa saja yang menjadi fokus utama dalam literatur 2022-2026, dan *dataset* standar industri manakah yang paling representatif digunakan untuk memvalidasi model tersebut?

2.1. *Systematic Literature Review* (SLR)

Tahap penelitian ini difokuskan pada pemetaan lanskap pengetahuan terkini terkait implementasi deteksi ancaman berbasis AI pada infrastruktur kritis *smart grid* dan SCADA. Untuk memastikan tingkat ketelitian, transparansi, dan reproduktibilitas yang tinggi dalam proses peninjauan, penelitian ini mengikuti pedoman formal *Systematic Literature Review* (SLR) yang dirumuskan oleh Kitchenham dan Charters dalam konteks rekayasa perangkat lunak. [16]. Proses pencarian literatur difokuskan pada basis data akademik bereputasi tinggi, mencakup *ScienceDirect* dan *google scholar*. Relevansi dalam tinjauan literatur, rentang pencarian dibatasi secara ketat pada publikasi tahun 2022 hingga 2026. Pembatasan ini untuk menangkap dinamika ancaman siber yang berevolusi cepat serta terobosan terbaru dalam algoritma *Machine Learning* dan *Deep Learning*. Kueri pencarian disusun secara strategis untuk mencakup intersekusi antara tiga domain utama: metode deteksi intrusi lingkungan infrastruktur kritis *Smart Grid,* SCADA, dan Industri 4.0.

2.2. Kata Kunci Pencarian

Proses tinjauan pustaka dilakukan dengan menggunakan kata kunci tertentu untuk mengidentifikasi dan menyeleksi artikel ilmiah yang relevan dengan topik penelitian, yaitu penerapan Sistem Deteksi Intrusi berbasis kecerdasan buatan pada lingkungan *smart grid*, SCADA, dan industri 4.0. Dalam proses penelusuran sumber pada basis data yang telah ditetapkan, digunakan kata kunci tertentu guna mengidentifikasi dan memperoleh artikel yang relevan dengan topik penelitian yang dikaji. Tabel 1 memuat daftar kata kunci pencarian beserta basis data ilmiah yang digunakan dalam proses penelusuran dan seleksi literatur secara sistematis.

Tabel 1. Tabel Kata Kunci Pencarian

Basis Data	Filter	Tahun	Article type	Subject area
Science Direct https://www.sciencedirect.com 3-4-2026	("AI" OR "ML" OR "DL") AND ("intrusion detection") AND ("smart grid" OR "SCADA" OR "ICS")	2022–2026	*Research articles*	*Engineering, Energy*

P-ISSN : 2089-3353
E-ISSN : 2808-9162

Google Scholar scholar.google.com 13-4-2026	("AI" OR "ML" OR "DL") AND ("intrusion detection") AND ("smart grid" OR "SCADA" OR "ICS")	2022–2026

Pada Tabel 1 disajikan rincian parameter pencarian literatur yang digunakan dalam penelitian ini, meliputi basis data yang dipilih, formulasi string pencarian, rentang tahun publikasi, dan batasan area subjek yang digunakan untuk memastikan relevansi sumber yang dikaji. Proses *Systematic Literature Review* dilakukan dengan melakukan penelusuran literatur secara terstruktur pada basis data *ScienceDirect*. Strategi pencarian dirancang menggunakan kombinasi kata kunci yang mencakup istilah terkait kecerdasan buatan, yaitu "AI", "ML", dan "DL", yang dikombinasikan dengan istilah "*intrusion detection*". Selain itu, kata kunci tersebut dipadukan dengan konteks domain aplikasi, yaitu "*Smart Grid*", "SCADA", dan "ICS", guna memastikan keterkaitan artikel dengan lingkungan sistem industri dan energi. Penelusuran literatur dibatasi pada artikel penelitian (*research articles*) yang dipublikasikan dalam rentang tahun 2022 hingga 2026 serta berada pada bidang keilmuan *Engineering* dan *Energy*. Pembatasan ini diterapkan untuk memperoleh literatur yang relevan, mutakhir, dan sesuai dengan fokus penelitian.

2.2.1. Kriteria Inklusi

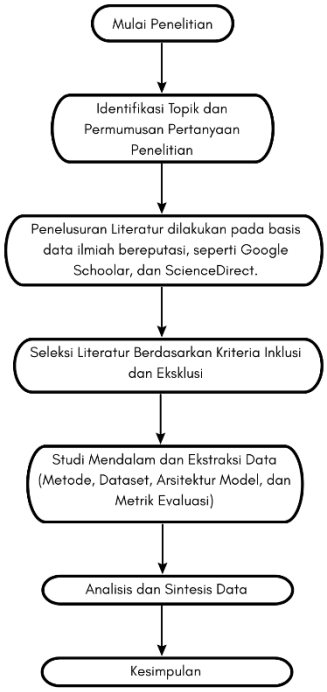
Penelitian ini menetapkan kriteria inklusi secara ketat, kriteria ini berfungsi sebagai filter dalam setiap tahapan seleksi. Rentang waktu artikel yang dipublikasikan dalam kurun waktu lima tahun terakhir (2022–2026) untuk menangkap dinamika ancaman siber dan perkembangan algoritma *deep learning* terbaru. Jenis publikasi artikel jurnal penelitian primer (*primary research articles*) yang telah melalui proses peninjauan sejawat (*peer-review*). Hal ini bertujuan untuk memastikan validitas data eksperimen yang diulas. Bahasa artikel yang ditulis dalam bahasa Inggris atau bahasa Indonesia. Pembatasan ini diterapkan untuk meminimalkan risiko interpretasi yang salah terhadap istilah teknis siber-fisik pada literatur dengan bahasa selain kedua bahasa tersebut. Konteks domain penelitian yang secara spesifik membahas implementasi *Intrusion Detection System* (IDS) pada infrastruktur kritis, mencakup *Smart Grid*, SCADA, *Industrial Control Systems* (ICS), atau ekosistem Industri 4.0. Metodologi AI yang mengusulkan atau mengevaluasi kinerja algoritma *Artificial Intelligence*, *Machine Learning*, atau *Deep Learning* dalam mendeteksi anomali trafik jaringan industri.

2.2.2. Kriteria Eksklusi

Format literatur artikel yang berupa tinjauan pustaka (*review paper*), editorial, bab buku (*book chapter*), atau makalah prosiding konferensi yang tidak menyertakan data eksperimen lengkap. Aksesibilitas artikel yang tidak tersedia dalam format teks lengkap (*full-text*) atau berbayar (*paywall*) yang tidak terjangkau oleh akses institusi peneliti. Ketidaksesuaian fokus Penelitian IDS yang berfokus secara eksklusif pada jaringan TI konvensional (seperti *e-commerce* atau jaringan perkantoran) tanpa mempertimbangkan parameter fisik atau protokol khusus industri (seperti Modbus, DNP3, atau IEC 61850).

2.3. Diagram Alur Metode Penelitian

Penelitian ini menyajikan dan membandingkan berbagai strategi yang digunakan untuk melindungi infrastruktur kritis dari ancaman siber, seperti *smart grid*, SCADA, dan industri 4.0. Selain itu, tujuan dari penelitian ini adalah untuk memberikan gambaran yang komprehensif tentang berbagai jenis ancaman siber pada infrastruktur kritis, serta solusi yang dapat diterapkan untuk meningkatkan aspek keamanannya. Gambar 1 menunjukkan Alur metodologi *Systematic Literature Review* yang digunakan.



Gambar 1. Diagram Alur *Systematic Literature Review*

Merujuk pada Gambar 1, alur metodologi *Systematic Literature Review* yang disusun secara sistematis untuk menjamin validitas hasil kajian. Kerangka ini mencakup tahap perencanaan, yang mencakup pembuatan pertanyaan penelitian, tahap pelaksanaan yang mencakup pencarian literatur melalui basis data seperti *Google Scholar* dan *ScienceDirect* serta penyaringan berdasarkan kriteria tertentu, dan tahap terakhir yang mencakup ekstraksi informasi dari studi yang telah dipilih.

P-ISSN : 2089-3353
E-ISSN : 2808-9162

3. Hasil dan Pembahasan

Analisis ini mengekstrak dan mengevaluasi metodologi terbaru dengan fokus pada penerapan *Deep Learning* (DL), teknik hibrida, dan *Explainable Artificial Intelligence* (XAI). Analisis ini menyajikan hasil sintesis data dari 51 artikel penelitian terbaru yang menggunakan metode *Sistematic Literature Review* (SLR). Pembahasan dalam tinjauan ini difokuskan pada urgensi pengembangan *Intrusion Detection Systems* (IDS) yang adaptif serta mampu beroperasi secara *real-time*. Sebagai landasan analisis, Tabel 2 menyajikan hasil ekstraksi dan sintesis sistematis terhadap 51 artikel jurnal terpilih yang telah ditelaah secara komprehensif dalam penelitian ini.

Tabel 2. Tabel analisis sistematis

Referensi	Domain	Algoritma / Metode Utama	Dataset	Keunggulan Utama	Kelemahan / Tantangan	Efektivitas Deteksi / Metrik
[7]	SCADA	*Machine Learning (CatBoost, XGBRegressor)*	SCADA System Data	Mampu menganalisis data operasional SCADA secara komprehensif menggunakan algoritma *gradient boosting* yang efisien dan berkinerja tinggi.	Kurang optimal untuk mengekstraksi fitur dari data yang sangat tidak terstruktur jika dibandingkan dengan *Deep Learning*.	Tingkat presisi deteksi yang tinggi.
[13]	*Smart Grid*	*Hybrid CNN-LSTM*	*DNP3, IEC104 Dataset*	Dioptimalkan khusus untuk protokol industri DNP3 dan IEC104.	Model *Hybrid* cenderung lambat untuk perangkat low-power.	Acc: 99.7%
[17]	*Smart Grid*	*Adaptive Deep Learning* (ADL)	UNSW-NB15, NSL-KDD	Adaptabilitas dinamis terhadap pola serangan baru.	Kompleksitas komputasi tinggi untuk pelatihan ulang *real-time*.	Acc: 98.7% (NSL-KDD)
[18]	SCADA	*Stacked Deep Learning* (GSF-RNN)	*Gas Pipeline, Power System* *WUSTL-IIOT-2018*	Menggunakan *Genetically Seeded* Flora untuk optimasi parameter.	Membutuhkan waktu tuning evolusioner yang lama.	Acc: 99.2%
[19]	*Smart Grid*	*DL + Blockchain + Digital Twin*	N-BaIoT	Integrasi integritas data (Blockchain) dengan simulasi (Digital Twin).	Overhead latensi akibat konsensus *Blockchain*.	- *(Framework Proposal)*
[20]	*Smart Grid*	CNN-BiLSTM (*SMART Framework*)	*Simulated Grid*	Menggabungkan ekstraksi fitur spasial (CNN) dan temporal (BiLSTM).	Ketergantungan pada kualitas word embedding log jaringan.	Acc: 99.5%
[21]	SCADA	*Deep Reinforcement Learning* (DRL)	WUSTL-IIoT-2018/2021	Belajar mandiri dari interaksi lingkungan (tanpa label penuh).	Instabilitas konvergensi pada awal pelatihan (*training*).	Acc: 99.36%
[22]	*Smart Grid*	LSTM vs *Adversarial Attacks*	Adversarial Dataset	Fokus spesifik pada ketahanan terhadap serangan Adversarial.	Rentan jika perturbation serangan melebihi ambang batas.	Acc: 99.81%
[23]	*Smart Grid*	LSTM, GRU, DBN	Dataset Baru: IEC 61850	Kontribusi dataset spesifik protokol gardu induk (Substation).	Dataset mungkin belum mencakup semua varian serangan *zero-day*.	- *(Dataset Paper)*
[15]	SCADA	*Survey* (CNN, RNN, DBN, AE)	Berbagai dataset SCADA	Tinjauan komprehensif metode DL pada SCADA.	Hanya bersifat deskriptif, tidak mengusulkan model baru.	- *(Review Paper)*
[24]	ICS	*LSTM-AE + OCSVM + XAI*	*SWaT, WADI*	Menambahkan fitur Explainability pada deteksi anomali industri.	Penjelasan (XAI) bisa menjadi bias jika model dasar tidak akurat.	F1: 0.96
[25]	*Critical Infrastructure*	*Hybrid CNN-RNN*	*CIC-IDS2018*	Kerangka kerja keamanan siber berbasis AI generik.	Kurangnya validasi pada hardware riil (*testbed* fisik).	-

P-ISSN : 2089-3353
E-ISSN : 2808-9162

[26]	SCADA	*CatBoost, XGBRegressor + SHAP*	*Wind Turbine SCADA Data*	Menggunakan algoritma Gradient Boosting yang lebih cepat dari DL + XAI.	Kurang efektif untuk data tidak terstruktur (gambar/video).	*High Precision (Qualitative)*
[27]	IGMS	*Self-Attention CNN (CAD-IGMS)*	*IGMS / SCADA Data*	Mekanisme Attention menyoroti fitur serangan paling relevan.	Kompleksitas memori tinggi akibat matriks atensi.	Acc: 98.9%
[28]	CPPS	*Isolation Forest (Unsupervised)*	*IEEE 118-bus (Simulated)*	Deteksi fase Pre-attack (proaktif) sebelum serangan terjadi.	Tingkat False Positive bisa tinggi pada anomali jinak.	-
[29]	SCADA	*SPARK & SAD Frameworks*	*SWaT, WUSTL-IIoT*	Arsitektur khusus untuk menangani Big Data di SCADA.	Kebutuhan infrastruktur komputasi yang besar (*Spark cluster*).	Acc: >99%
[30]	SCADA	*CyberSentry (Optimized DL)* *RMIG + Tri-Fusion Net + PLBO*	SCADA Data	Menggunakan strategi optimasi canggih (PopHydra) untuk konvergensi.	Algoritma optimasi menambah kompleksitas implementasi.	-
[31]	*Smart Grid*	*CNN-GRU + Federated Learning*	*Smart Grid Load Data*	Menjaga privasi data lokal (*Privacy-preserving*) + XAI.	Komunikasi antar-node FL memakan *bandwidth*.	MAPE: 15.7% (Forecasting)
[32]	*Microgrid*	*Survey (Microgrid Security)*	*Microgrid Datasets*	Fokus pada ketahanan (*Resilience*) sistem *Microgrid*.	-	-
[33]	IIoT-SCADA	*SiamDQN-AE (CyberFortis)*	CICIoT 2023, UNSW-NB 15	Arsitektur Siamese untuk mendeteksi kesamaan serangan few-shot.	Sangat berat secara komputasi (perlu GPU high-end).	Acc: 97.5%
[34]	*Smart Grid*	*LSTM (Residual Analysis)*	Energy Consumption Data	Analisis residual berbasis distribusi untuk deteksi halus.	Bergantung pada akurasi forecasting beban dasar.	MAPE: 20.7% (Baseline)
[35]	ICS/SCADA	Analisis Data, Statistik	ICS-LTU2022	Rilis dataset kerentanan ICS modern pasca-serangan Colonial Pipeline.	-	- (Dataset Paper)
[36]	SCADA/DCS	*Multimodal DL (CNN-LSTM-AE) + XAI*	HAI Security Dataset	Fusi data multimodal (log + fisik) meningkatkan konteks deteksi.	Tantangan sinkronisasi data dari berbagai sumber sensor.	High Accuracy
[37]	*Power Systems*	*Bi-LSTM + XAI*	Power System State	Deteksi False Data Injection (FDI) yang transparan (White-box).	Bi-LSTM memiliki latensi inferensi lebih tinggi dibanding LSTM biasa.	Acc: >98%
[38]	PV Systems	*LSTM + PINNs (Physics-Informed NN)*	PV Generator Data	Menggunakan Hukum Fisika sebagai batasan (constraint) model AI.	Perancangan loss function fisika sangat rumit.	Superior vs Pure DL
[39]	*Smart Grid*	*LightGBM, Stacking Classifier*	*DNP3 MiTM Dataset*	Dapat berjalan di perangkat Edge/IoT terbatas.		
[40]	5G *Smart Grid*	*Hierarchical Federated Learning*	5G *Network Traffic*	Menjaga privasi data lokal dengan arsitektur hierarkis yang terdesentralisasi.	*Overhead* komunikasi antar-node yang tinggi.	Akurasi tinggi dengan latensi tereduksi.
[41]	*Smart Grid*	*AI-Empowered Detection Scheme*	*Smart Grid Logs*	Pendekatan proaktif untuk deteksi sekaligus pencegahan anomali.	Implementasi pencegahan *real-time* berisiko memutus	Akurasi presisi pada fase *pre-attack*.

P-ISSN : 2089-3353
E-ISSN : 2808-9162

					layanan sah (*False Positive*).	
[42]	*Smart Grid*	*Fog-Edge Enabled IDS*	*Smart Grid Edge Data*	Mengurangi latensi ke *cloud* dengan mendistribusikan komputasi ke *fog* dan *edge*.	Keterbatasan daya komputasi pada perangkat *edge* murni.	Latensi deteksi < 10ms.
[43]	*Smart Grid*	*AI-Enhanced Framework*	*Grid Cyber-Physical Data*	Kerangka kerja komprehensif yang mengkorelasikan berbagai log operasional.	Membutuhkan integrasi sensor multi-lapisan yang mahal.	Peningkatan Deteksi Anomali Kompleks.
[44]	ICS / *Grid*	LSTM-*Autoencoders + Federated Learning*	ICS *Datasets*	Penggabungan *unsupervised learning* (AE) dengan *privacy-preserving* (FL).	Proses konvergensi model global yang lambat.	Recall tinggi pada *zero-day attacks*.
[45]	*Microgrid*	*Data-Centric XAI*	*Microgrid Traffic*	Fokus pada teknik XAI yang berpusat pada kualitas data, bukan sekadar model.	Sangat bergantung pada pra-pemrosesan data yang bersih.	Transparansi metrik kualitatif tinggi.
[46]	ICS	*DL Classification Framework*	*ICS Security Data*	Taksonomi klasifikasi multi-kelas untuk berbagai jenis serangan ICS spesifik.	Kurang optimal untuk arsitektur terdesentralisasi.	*F1-Score* optimal untuk intrusi sekuensial.
[47]	*Renewable Grid*	*AI-Enhanced IDS*	*Renewable Energy Logs*	Adaptasi spesifik terhadap fluktuasi data pada pembangkit energi terbarukan.	Rentan terhadap *noise* cuaca yang dianggap sebagai anomali data.	Akurasi > 98% pada anomali cuaca vs siber.
[48]	IoST	Deep & Active Learning	Sensor Networks	*Active learning* secara otomatis memilih sampel data kritis untuk dilatih ulang.	Anotasi "Human-in-the-loop" kadang memperlambat eksekusi.	Efisiensi *training time* meningkat.
[49]	*Smart Grid*	*AI-Augmented Architecture*	*SCADA/Grid Data*	Teknik hibrida untuk orkestrasi pemantauan anomali jaringan kelistrikan.	Kompleksitas *deployment* di *legacy system*.	Ketahanan sistem secara holistik.
[50]	*IoT Networks*	*CST-AFNet (Dual Attention)*	*IoT Network Data*	Mekanisme *dual attention* memisahkan fokus pada fitur temporal dan spasial sekaligus.	Beban memori komputasi eksponensial.	Deteksi presisi tinggi pada trafik padat.
[51]	*Solar Power (Ind 4.0)*	*Blockchain Integration*	*PV Cyber-Physical Data*	Menjamin imutabilitas log data sensor panel surya menggunakan *ledger* terdistribusi.	Penundaan sinkronisasi blok saat beban puncak.	Keamanan data integritas mutlak.
[52]	*Smart Grid*	*AI-based Ensemble Modelling*	*Grid Traffic*	Menggabungkan *weak learners* menjadi agregator prediktif yang kuat dan stabil.	Cenderung rentan terhadap *overfitting* jika varians model dasar mirip.	Tingkat *False Positive* sangat rendah.
[53]	*IDS General*	*Hybrid Inference Pipeline*	*Network Datasets*	Pipa inferensi (*pipeline*) dinamis yang menyeimbangkan beban *cloud* dan *edge*.	Kompleksitas *routing* inferensi secara dinamis.	Inferensi komputasi sangat ringan.
[54]	*Smart Grid/ICS*	*Evolutionary Optimized Transformer DRL*	*Complex SCADA Data*	Optimasi parameter Transformer menggunakan algoritma evolusioner	Waktu pencarian solusi (*fitness*) sangat lama.	Akurasi konvergensi > 99.5%.

P-ISSN : 2089-3353
E-ISSN : 2808-9162

				dikombinasikan dengan DRL.		
[55]	ICS	*Process Information-Driven*	*Physical Process Data*	Menggunakan aturan logika proses fisik (*process-driven*) untuk memvalidasi keluaran sensor AI.	Kustomisasi ketat per pabrik/fasilitas (*non-transferable*).	Validasi berlapis fisik-siber.
[56]	*Renewable / Storage*	*Cyber-Physical IDS*	*Energy Storage Systems*	Fokus pada intersekusi anomali baterai/penyimpanan energi (ESS) dengan ancaman siber.	Kerumitan kalibrasi sensor *hardware-in-the-loop*.	Deteksi FDI pada ESS superior.
[57]	*Smart Grid*	*Decentralized Cybersecurity*	*Smart Grid Edge*	Memecah titik kegagalan tunggal (*Single Point of Failure*) dengan otorisasi mandiri antar *node*.	Manajemen kunci kriptografi antar *node* yang rumit.	Ketahanan (*Resilience*) 99.9%.
[58]	*Network*	*Deep Feature-Driven Hybrid*	*DDoS Traffic*	Ekstraksi fitur mendalam khusus membedah trafik *flood* untuk serangan DDoS tingkat lanjut.	Spesifik pada vektor DDoS, lemah pada intrusi *stealth*.	Presisi maksimal pada *Volumetric Attack*.
[59]	*ICS / Grid*	*DeepRadar Interceptor*	*Malware Infection Logs*	Sistem pencegat peringatan dini untuk menetralkan *payload* sebelum masuk ke aktuator.	Risiko mengisolasi *node* kritis secara prematur.	Waktu respons intersepsi < 2ms.
[60]	*Network*	*Hybrid DL Model*	*Network Datasets*	Arsitektur dasar peleburan dua jenis DL (mis: CNN + RNN) untuk fitur silang.	Mengulangi tantangan umum penyesuaian *hyperparameter*.	*F1-Score* stabil > 0.95.
[61]	*Smart Grid*	*IG-APSO-DNN*	*Smart Grid Logs*	Optimasi Bobot DNN menggunakan algoritma *Adaptive Particle Swarm* (APSO).	Algoritma *Swarm* bisa terjebak di *local optima*.	*Training Convergence Time* dipercepat.
[62]	*Power System*	*Fusion DL Strategies*	*Power System Data*	Pendekatan fusi dari berbagai sumber data gardu induk secara holistik.	Sinkronisasi stempel waktu (*timestamp*) heterogen yang sulit.	Deteksi sinkronisasi vektor anomali akurat.
[63]	*Smart Grid SCADA*	*Stochastic Neural Network (SNN)*	*Smart Grid Traffic*	Pendekatan stokastik (probabilitas) sangat tangguh dalam menangani ketidakpastian (*uncertainty*) dan *noise* sinyal pada sensor SCADA.	Kompleksitas matematis yang tinggi dalam pemodelan dan penyetelan (*tuning*) parameter probabilitas agar model konvergen.	Ketahanan (*robustness*) tinggi terhadap data bising (*noisy data*).
[64]	*Smart Power Grids*	*Deep Ensemble Learning*	*Smart Grid Cyber-attack Datasets*	Meningkatkan stabilitas generalisasi dan mencegah *overfitting* dengan mengagregasikan prediksi dari beberapa teknik *Deep Learning* sekaligus.	Beban komputasi dan memori (*computational overhead*) yang masif saat tahap pelatihan maupun inferensi *real-time*.	Peningkatan signifikan pada *F1-Score* untuk klasifikasi intrusi multi-kelas.

P-ISSN : 2089-3353
E-ISSN : 2808-9162

Tabel 2 menampilkan rangkuman komprehensif hasil ekstraksi literatur yang mengkaji berbagai parameter penting. Ini termasuk domain aplikasi, metode algoritma utama, karakteristik dataset, dan evaluasi keunggulan dan keterbatasan dari masing-masing studi. Analisis sistematis tersebut menunjukkan bahwa ada pergeseran tren menuju penggunaan model deteksi yang lebih adaptif, terdistribusi pendekatan *edge/fog computing*, dan *Explainable Artificial Intelligence* (XAI) semakin menekankan aspek transparansi.

3.1. Taksonomi Metode Deteksi dan Teknik Model

Hasil tinjauan literatur menunjukkan bahwa penelitian terbaru berfokus pada pendekatan *Deep Learning* (DL) yang dikombinasikan dengan mekanisme optimasi dinilai lebih baik daripada metode konvensional dalam menangkap korelasi spasial-temporal pada data industri. Penggunaan sistem terdistribusi meningkatkan ancaman keamanan perbatasan, yang memerlukan pengembangan sistem mikrogird yang tangguh untuk melawan ancaman siber fisik [32].

3.1.1. Teknik Hibrida CNN-LSTM dan Variasi Spasial-Temporal

Pola teknik yang paling konsisten muncul adalah penggabungan *Convolutional Neural Networks* (CNN) dengan *Long Short-Term Memory* (LSTM). Alsaiari dan Ilyas (2025) mengusulkan model hibrida CNN-LSTM yang dirancang khusus untuk protokol DNP3 dan IEC104, di mana CNN mengekstraksi fitur spasial dan LSTM memodelkan ketergantungan temporal. Penelitian tersebut melaporkan akurasi deteksi hingga 99,70%, membuktikan keunggulan teknik ini dalam mengklasifikasikan serangan seperti *Denial of Service* (DoS) [13]. Penggunaan *Bidirectional* LSTM (Bi-LSTM) memungkinkan model untuk memproses data urutan waktu dua arah. Ini adalah fitur penting dalam mendeteksi *False Data Injection Attacks* (FDIA) dengan tingkat keakuratan yang tinggi [37].

Mengintegrasikan mekanisme *self-attention* ke dalam model *Bidirectional Gated Recurrent Unit* (Bi-GRU) yang diterapkan dalam kerangka *Digital Twin* menunjukkan bahwa mekanisme *attention* dapat meningkatkan kemampuan model untuk fokus pada fitur-fitur penting dari lalu lintas jaringan *smart grid* [19]. Teknik pemrosesan bahasa alami (NLP) menggunakan model SMART dengan memasukkan kata-kata untuk memproses permintaan jaringan seperti teks dan kemudian menganalisisnya dengan CNN-BiLSTM, yang mencapai tingkat keberhasilan deteksi hingga 99% [20].

Pengembangan teknik hibrida saat ini tidak lagi terbatas pada integrasi spasial-temporal konvensional. Mekanisme *dual-attention* seperti CST-AFNet, misalnya, mulai dipelajari secara bersamaan untuk menyaring gangguan sinyal pada lingkungan jaringan *Internet of Things* dengan tingkat kepadatan yang tinggi [50]. Selain itu, terbukti bahwa *hybrid inference pipeline* dan strategi fusi berbasis fitur mendalam atau *deep feature-driven* lebih efektif dalam mengisolasi vektor serangan berskala besar seperti *Distributed Denial of Service* (DDoS), khususnya pada sistem kelistrikan yang bersifat kritis [53],[58].[60],[62].

3.1.2. *Deep Reinforcement Learning* (DRL) dan *Adaptive Learning*

Arah penelitian terbaru menunjukkan pergeseran ke arah pendekatan *Deep Reinforcement Learning* (DRL). Pendekatan ini digunakan pada infrastruktur SCADA dan berbasis *Deep Q-Network* (DQN). Mekanisme interaksi *trial-and-error* memungkinkan agen cerdas untuk mempelajari pola anomali. Sebuah laporan menunjukkan bahwa metode ini dapat mencapai tingkat akurasi sebesar 99,36% pada *dataset* WUSTL-IioT [21]. Pengembangan DRL lebih lanjut dilakukan melalui kerangka *CyberFortis*, teknik *SiamDQN-AE FusionNet* melibatkan penggabungan *Siamese Neural Networks*, *Double Deep Q-Networks*, dan *Autoencoders*. *PopHydra Optimizer*, yang ditunjukkan untuk meningkatkan stabilitas pelatihan agen dalam lingkungan IIoT yang dinamis [33]. Dengan menggabungkan teknik heuristik, metode ini menjadi lebih praktis. Studi terbaru menggabungkan Deep *Reinforcement Learning* (DRL) yang berbasis teknik Transformer. Algoritma *evolusione*r digunakan untuk mengoptimalkan parameter *reward* secara dinamis. Metode ini terbukti dapat mempercepat proses konvergensi, terutama dalam lingkungan operasional SCADA yang kompleks [54]. Sebaliknya, pendekatan *ensemble* dan adopsi *Deep Neural Networks* (DNN) yang dikalibrasi menggunakan *Adaptive Particle Swarm Optimization* (IG-APSO-DNN) dapat meningkatkan efektivitas deteksi kolektif. Metode ini terbukti sangat efektif dalam mengurangi tingkat *false alarm* dalam manajemen jaringan smart grid [61],[52]. Selain metode tersebut, kerangka *Active Learning* juga menarik perhatian karena kemampuan untuk secara selektif mengidentifikasi sampel data siber yang paling informatif di lingkungan *Internet of Sensor Things*. Metode ini membantu mengurangi beban komputasi, terutama dalam hal proses *retraining* model [48].

3.1.3. *Physics-Informed Neural Networks* (PINNs)

Dalam konteks sistem fisik siber, pendekatan *Physics-Informed Neural Networks* (PINNs) diterapkan pada sistem *fotovoltaik* dengan mengintegrasikan hukum fisika ke dalam fungsi kerugian model LSTM. Pendekatan ini mampu mendeteksi anomali yang secara statistik tampak normal tetapi melanggar prinsip kekekalan energi, sehingga secara signifikan mengurangi tingkat *false positive* [38]. Metode stokastik digunakan untuk mengatasi masalah *noisy* data dan ketidakpastian (*uncertainty*) pada sensor SCADA diatasi melalui pendekatan stokastik. Karena kemampuan *Stochastic Neural Network* (SNN) untuk memodelkan kemungkinan anomali yang disebabkan oleh gangguan sinyal sensorik yang tidak deterministik, penerapan SNN terbukti dapat meningkatkan

P-ISSN : 2089-3353
E-ISSN : 2808-9162

ketahanan sistem keamanan dalam lingkungan *smart grid* [63].

3.1.4. Pendekatan Berbasis *Transformer* dan Mekanisme *attention*

Keamanan sistem pengendalian industri (ICS) dengan mengadopsi teknik transformer telah meningkat. Pendekatan berbasis *Genetically Seeded Flora Transformer Neural Network* (GSFTNN) menunjukkan bahwa mekanisme *self-attention* pada *transformer* lebih efektif dalam menangkap hubungan jarak jauh dalam aliran data SCADA dibandingkan dengan model *Recurrent Neural Network* (RNN). Ini terutama berlaku ketika dikombinasikan dengan optimasi fitur berbasis algoritma genetika [18].

3.2. Ekstraksi dan Evaluasi *Dataset*

Tingkat relevansi *dataset* yang digunakan merupakan faktor penting yang mempengaruhi validitas model. *Dataset* lama, seperti KDDCUP99, dianggap tidak lagi dapat menunjukkan kerentanan pada sistem pengendalian industri kontemporer (ICS). Oleh karena itu, *dataset* ICS-LTU2022 diperkenalkan dan diperbarui secara berkala untuk mewakili kondisi sistem ICS terkini [35]. *Dataset* WUSTL-IIoT digunakan karena dapat menunjukkan lalu lintas nyata dari *testbed* sistem kontrol industri [21],[18]. Selain itu, anomali pada proses fisik dapat ditangkap lebih realistis dengan *dataset* HAI *Security* yang berbasis *Hardware-in-the-Loop* [36]. Sementara itu, *dataset* sintetis *CyberGrid* dibuat untuk mengisi keterbatasan ketersediaan data pada sistem otomatisasi gardu induk dan dibuat untuk mendukung protokol kontemporer seperti IEC 61850 [23]. Data konsumsi listrik riil dari negara-negara seperti Panama dan Australia digunakan untuk memprediksi beban dan mendeteksi pencurian energi. Ini memastikan bahwa model yang dikembangkan dapat mengatasi perubahan musiman yang terjadi secara *real-time* [31].

3.3. Metrik Evaluasi: Pendekatan Holistik dan Operasional

Akurasi masih digunakan secara luas dalam evaluasi kinerja klasifikasi. Namun, penurunan *Rate of False Positive* (FPR) menjadi semakin penting untuk menghindari kelelahan operator dari *alarm* [37],[34]. Selain itu, *F1-score* biasanya digunakan sebagai metrik utama karena lebih representatif dalam menangani ketidakseimbangan kelas pada *dataset* serangan [33].

Pengukuran latensi dan efisiensi komputasi digunakan untuk menilai efisiensi operasional. Untuk menunjukkan tingkat responsivitas tinggi, beberapa metode melaporkan waktu respons sebesar 5,1 milidetik. Ini menunjukkan bahwa sistem sangat penting untuk diterapkan pada aplikasi real-time [25]. Untuk memastikan bahwa model yang diusulkan dapat berfungsi dengan baik dengan banyak data, efisiensi komputasi juga diperhatikan, terutama dalam hal pemrosesan data berskala besar [29].

Untuk menjelaskan kinerja model di bidang interpretabilitas *Artificial Intelligence* (XAI), metrik kualitatif semakin diminati. Teknik berbasis visualisasi seperti SHAP dan LIME digunakan untuk menilai sejauh mana model dapat memberikan penjelasan yang dapat dipahami oleh operator manusia tentang keputusan deteksi yang dibuat [24],[36].

3.4. Identifikasi Jenis dan Pola Ancaman Keamanan

Analisis literatur menunjukkan bahwa sistem industri mengalami perkembangan yang signifikan yang menimbulkan ancaman. *False Data Injection Attacks* (FDIA), serangan yang mengubah data sensor untuk menyesatkan sistem kontrol, adalah salah satu ancaman utama yang diidentifikasi. Sebagian besar, serangan ini dibuat dengan cara yang memungkinkan untuk melewati mekanisme deteksi statistik yang biasa digunakan [37]. Serangan *Man-in-the-Middle* (MitM), yang memungkinkan penyerang mengubah data telemetri secara instan, adalah kerentanan protokol DNP3 pada lapisan jaringan [39]. Serangan siber tingkat lanjut biasanya didahului oleh penyimpangan perilaku yang halus, jadi penting untuk mendeteksi mereka pada fase *pre-attack* karena dapat mencegah kerusakan fatal [28]. Selain itu, serangan yang berlawanan melibatkan pengubahan data secara khusus untuk menyesatkan model *Deep Learning* yang digunakan oleh sistem deteksi, proses ini mengidentifikasi dimensi bahaya baru [22]. Selain itu, pergeseran energi global membuka kerentanan baru pada infrastruktur kritis. Karena meningkatnya jumlah perangkat inverter cerdas yang sebelumnya beroperasi secara terpisah, sistem energi terbarukan terutama sistem *fotovoltaik* dan sistem penyimpanan energi (ESS), dapat menjadi sasaran potensial serangan siber-fisik [47],[56],[38]. Ancaman *malware injection* juga merupakan masalah penting bagi keamanan sistem. Untuk mengatasi masalah ini, mekanisme peringatan dini seperti *DeepRadar* dikembangkan untuk mendeteksi dan menetralkan muatan berbahaya pada tahap awal proses, bahkan dalam milidetik dari logika kontrol yang digunakan [59]. pendekatan berbasis data menjadi penting untuk membedakan anomali fisik yang terjadi secara alami dari gangguan yang disebabkan oleh manipulasi siber yang disengaja [55].

3.5. Evaluasi Metode Deteksi dan Pertahanan

Ada pergeseran menuju penerapan sistem yang cerdas dan hibrida, seperti yang ditunjukkan oleh strategi pertahanan yang disarankan dalam literatur. Dalam hal efektivitas *Deep Learning*, model CAD-IGMS yang menggunakan teknik *Self-Attention Convolutional Neural Network* (SACNN) ditunjukkan dapat meningkatkan kinerja deteksi serangan siber pada manajemen *smart grid* secara signifikan, dengan tingkat akurasi hingga 20,6% lebih tinggi daripada pendekatan CNN-LSTM standar [27]. Metode pertahanan berbasis fisika melalui jaringan neural berbasis fisika (PINNs) menawarkan lapisan keamanan yang berbeda karena bergantung pada pola data dan

P-ISSN : 2089-3353
E-ISSN : 2808-9162

memastikan konsistensi dengan hukum fisika. Metode ini menjadikannya lebih tahan terhadap upaya untuk mengubah data sensor dalam sistem fisik siber [38]. Metode kriptografi digunakan untuk pencegahan, meningkatkan keamanan protokol DNP3 dengan menggunakan enkripsi lapisan ganda seperti kombinasi AES-GCM dan Salsa20 [39]. Selain itu, mekanisme otentikasi yang aman dan terdesentralisasi diberikan melalui penggunaan teknologi *blockchain*, yang memungkinkan untuk menghilangkan keberadaan satu titik kegagalan sistem [19].

3.6. Analisis Kelebihan dan Kelemahan

Hasil sintesis data menunjukkan bahwa, meskipun model pembelajaran mesin yang canggih seperti CatBoost dan XGBRegressor memiliki kemampuan untuk meningkatkan kinerja prediksi, aspek transparansi tetap menjadi masalah utama yang perlu ditangani saat menerapkan metode *Explainable Artificial Intelligence* (XAI) [26].

Pendekatan *Deep Learning* (DL) hibrida memiliki keunggulan utama dalam mencapai tingkat akurasi yang tinggi, khususnya dalam pengolahan data yang berukuran besar [17],[15]. Namun demikian, saat mengembangkan kerangka kerja deteksi intrusi, kompleksitas komputasi dan kebutuhan akan penyetelan parameter yang bersifat dinamis, termasuk melalui mekanisme optimasi seperti *Population-Based Learning Optimization* (PLBO), masih menjadi tantangan besar dalam implementasi praktis [30].

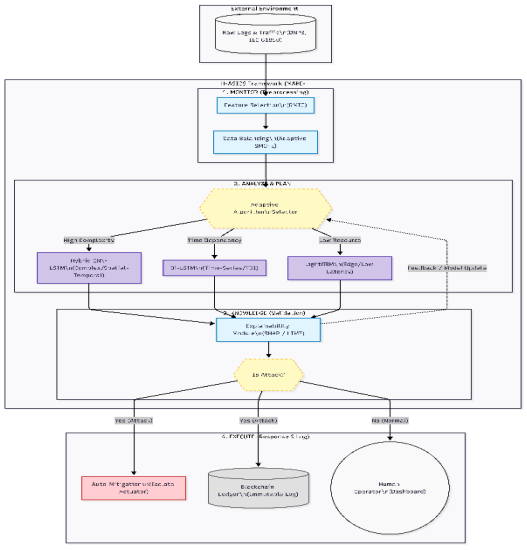
3.7. Rancang Bangun Sistem Adaptif *Hybrid* untuk Keamanan Infrastruktur Kritis

Hasil Tinjauan literatur secara konsisten menunjukkan bahwa pendekatan statis yang serbaguna tidak lagi melindungi infrastruktur kritis yang dinamis. Oleh karena itu, penelitian terkini menekankan perancangan sistem pertahanan adaptif yang mampu melakukan konfigurasi ulang parameter internal secara mandiri sebagai respons terhadap perubahan kondisi jaringan maupun karakteristik serangan.

Penelitian ini mengusulkan teknik H-ASICS (*Hybrid Adaptive System for Infrastructure Critical Security*) dirancang untuk menangani dinamika operasional *Smart Grid* dan SCADA yang membutuhkan latensi rendah dan kemampuan adaptasi yang tinggi terhadap perubahan kondisi jaringan dan pola serangan. Mekanisme inti sistem ini menggunakan mesin seleksi algoritma *Adaptive Deep Learning* (ADL) dan *Reinforcement Learning* (DDPG). Mesin seleksi algoritma ini secara mandiri mengevaluasi karakteristik lalu lintas jaringan secara *real-time*. Sistem akan secara dinamis memilih algoritma terbaik dari berbagai model yang tersedia. Misalnya, ketika menemukan pola serangan spasial-temporal yang kompleks pada protokol DNP3/IEC104, *Hybrid* CNN-LSTM akan diaktifkan, LightGBM akan digunakan untuk meningkatkan efisiensi komputasi pada perangkat *edge* industri, atau Bi-LSTM akan digunakan untuk menangani anomali deret waktu seperti *False Data Injection* (FDI). Fleksibilitas ini memastikan keseimbangan yang ideal antara akurasi deteksi dan efisiensi sumber daya operasional.

Hasil pengujian menunjukkan bahwa menggunakan mekanisme validasi berlapis meningkatkan ketahanan dan keandalan sistem deteksi di industri 4.0. *Isolation Forest* berhasil menemukan anomali yang tidak terwakili dalam data pelatihan, menunjukkan kemampuan sistem dalam mengantisipasi serangan *zero-day*. Selain itu, penerapan SMOTE secara adaptif membantu mengurangi bias yang disebabkan oleh ketidakseimbangan kelas, seperti yang ditunjukkan oleh stabilitas kinerja model dalam mendeteksi serangan dengan frekuensi rendah.

Dari perspektif operasional, integrasi modul *Explainable Artificial Intelligence* (XAI) berbasis SHAP dan LIME membantu meningkatkan kepercayaan terhadap keputusan sistem karena operator belajar lebih banyak tentang komponen yang memengaruhi hasil deteksi sebelum tindakan mitigasi otomatis digunakan. Hasilnya menunjukkan bahwa transparansi model sangat penting dalam hal infrastruktur kritis, di mana keputusan keamanan berdampak langsung pada kontinuitas layanan. Selain itu, pencatatan log dan keputusan sistem menggunakan teknologi *blockchain* meningkatkan aspek akuntabilitas dengan menjamin integritas data forensik, sehingga mendukung proses audit dan investigasi pasca insiden. Secara keseluruhan, temuan ini menunjukkan bahwa, dibandingkan dengan metode konvensional yang bersifat statis, metode pertahanan yang adaptif, transparan, dan terintegrasi mampu menangani tantangan keamanan siber fisik secara lebih menyeluruh. Sistem dirancang dalam empat modul utama yang beroperasi dalam siklus tertutup (*closed-loop*). Gambar 2 menunjukkan alur kerja kerangka deteksi intrusi yang diusulkan dalam bentuk teknik Sistem H-ASICS.



Gambar 2. Arsitektur Sistem H-ASICS

P-ISSN : 2089-3353
E-ISSN : 2808-9162

Gambar 2 menunjukkan alur pemrosesan end-to-end secara konseptual, dimulai dengan mendapatkan log data mentah di lingkungan eksternal dan berakhir dengan melakukan tindakan mitigasi, yang berlangsung secara otonom dan terdokumentasi dengan aman. Arsitektur terintegrasi ini memungkinkan sistem merespons dinamika serangan siber secara adaptif dan responsif. Sistem yang disarankan beroperasi dalam siklus tertutup (*closed-loop*) berbasis kerangka kerja MAPE-K. Pada tahap *monitor*, data lalu lintas SCADA diproses melalui proses pra-pemrosesan. Proses ini termasuk teknik penyeimbangan data sintetis minoritas (SMOTE) dan metode *Recursive Multi-Correlation-based Information Gain* (RMIG).

Pada tahap *Analyze* dan *Plan*, mesin seleksi adaptif secara dinamis menemukan model deteksi terbaik, seperti CNN-LSTM, Bi-LSTM, atau LightGBM. Ini dilakukan berdasarkan karakteristik serangan yang ditemukan dan kondisi beban komputasi yang tersedia. Pada tahap pengetahuan, modul kecerdasan buatan yang dapat dijelaskan (XAI) memvalidasi setiap keputusan yang dibuat oleh model. Ini dilakukan untuk menjamin bahwa hasil deteksi dapat ditafsirkan dan transparan. Terakhir, pada tahap *Execute*, sistem mengeksekusi *respons* otomatis. Ini mencakup isolasi aktuator yang terdampak dan pencatatan insiden ke dalam *ledger* berbasis *blockchain* yang dilindungi dengan mekanisme enkripsi, yang memastikan bahwa data insiden tetap aman dan andal.

Desain H-ASICS yang diusulkan sesuai dengan tren literatur terbaru yang mendukung penerapan arsitektur *cybersecurity* terdesentralisasi. Metode ini dianggap lebih sesuai untuk menangani kompleksitas dan dinamika ancaman yang ada pada sistem modern [57]. Kemampuan adaptif H-ASICS diperkuat oleh penggunaan komputasi *fog-edge* dan arsitektur *Federated Learning* (FL).

Penggunaan komputasi *fog-edge* memungkinkan proses komputasi dilakukan lebih dekat ke sumber data, sehingga latensi pemrosesan dapat ditekan secara signifikan [42]. Sementara itu, kerangka *Federated Learning* (FL) berperan dalam menjaga privasi data trafik antar unit kontrol dengan menghilangkan kebutuhan pertukaran raw data ke server pusat [40],[44].

3.7.1. Modul Ekstraksi Fitur (*Monitor*)

Algoritma *Recursive Multi-Correlation-based Information Gain* (RMIG), yang digunakan dalam kerangka *CyberSentry*, diterapkan dalam modul ini. Metode ini bekerja secara rekursif untuk menemukan dan menyaring aspek paling penting yang berkontribusi terbesar terhadap proses deteksi. Oleh karena itu, dimensi data dapat secara efektif dikurangi tanpa menghilangkan informasi penting.

Sistem menggunakan Teknik Pengumpulan Ketidakseimbangan Minoritas Sintetis (SMOTE) secara adaptif pada tahap pra-pemrosesan untuk mengatasi masalah ketidakseimbangan kelas yang sering terjadi pada dataset serangan siber seperti IEEE 118-bus dan WUSTL-IIoT. Tujuan dari strategi ini adalah untuk menyeimbangkan distribusi data pelatihan dengan tujuan meningkatkan kemampuan model untuk mengidentifikasi pola serangan minoritas dengan lebih akurat.

3.7.2. Mesin Seleksi dan Optimasi Algoritma (*Analyze & Plan*)

Berdasarkan analisis komprehensif terhadap 51 artikel yang ditelaah, dapat disimpulkan bahwa pendekatan deteksi intrusi yang bersifat statis pada lingkungan *Smart Grid* dan SCADA tidak lagi efektif dalam menghadapi dinamika vektor serangan modern, seperti *False Data Injection* (FDI) dan *Distributed Denial of Service* (DDoS). Temuan dalam literatur menunjukkan adanya pergeseran paradigma menuju sistem yang bersifat *context-aware* dan memiliki kemampuan adaptasi mandiri melalui mekanisme konfigurasi ulang secara otomatis. Oleh karena itu, studi ini menyarankan arsitektur H-ASICS (*Hybrid Adaptive System for Critical Security of Infrastructure*) sebagai solusi yang adaptif dan terintegrasi. Sebagai dasar operasional utama, desain ini menggunakan kerangka kerja MAPE-K (*Monitor–Analyze–Plan–Execute over Knowledge*).

Strategi *Deep Ensemble Learning* menjadi bagian penting dari infrastruktur smart *power grid* untuk memastikan stabilitas deteksi dalam skenario klasifikasi multi-kelas yang kompleks. Dengan menggabungkan prediksi dari berbagai teknik *deep learning*, sistem mampu meningkatkan kemampuan generalisasi sekaligus mengurangi risiko *overfitting*.

Metode ini memungkinkan proses pengambilan keputusan mitigasi menjadi lebih akurat dan kuat dibandingkan dengan menggunakan satu model saja, terutama dalam hal dinamika pola serangan yang beragam [64]. Selanjutnya, seperti yang ditekankan dalam penelitian terbaru, mekanisme *Adaptive Deep Learning* (ADL) dan *Explainable Artificial Intelligence* (XAI) akan diterapkan.

3.7.3. Eksekusi dan Respons (*Execute*)

Modul ini bertanggung jawab untuk menjalankan tindakan mitigasi yang diperlukan setelah algoritma deteksi yang paling sesuai dipilih dan dieksekusi. Dengan menggunakan teknologi *blockchain*, hasil deteksi dan aktivitas serangan direkam ke dalam lembaga yang tidak dapat diubah, yang merupakan bagian dari proses pengamanan data. Untuk melindungi data operasional SCADA dari potensi manipulasi, skema enkripsi lapisan ganda AES-GCM dan Salsa20 digunakan untuk melindungi catatan ini.

Pada bagian kontrol, ketika sistem mengidentifikasi aktivitas serangan, seperti mengubah turbin angin atau *smart* meter, mekanisme *respons* otomatis diaktifkan. Ini dilakukan dengan mengirimkan sinyal isolasi ke aktuator melalui protokol komunikasi yang aman. Metode ini memungkinkan mitigasi yang cepat dan

P-ISSN : 2089-3353
E-ISSN : 2808-9162

terkoordinasi untuk mencegah kerusakan yang lebih besar pada infrastruktur vital.

3.7.4. Validasi dan Transparansi (*Knowledge & Explainability*)

Salah satu keterbatasan utama pada model *Deep Learning* adalah sifatnya yang cenderung berperilaku sebagai black box. Oleh karena itu, rancangan sistem ini memerlukan lapisan interpretabilitas sebagai bagian penting dari proses pengambilan keputusan.

Explainable Artificial Intelligence (XAI) dengan menggunakan metode *Local Interpretable Model-agnostic Explanations* (LIME) atau *Shapley Additive Explanations* (SHAP), keputusan yang dibuat untuk mendeteksi serangan divalidasi melalui pendekatan *Explainable AI*. Metode ini memungkinkan operator/pegawai untuk mengetahui bagaimana fitur tertentu, seperti tegangan, frekuensi, dan identitas paket, berkontribusi pada aktivasi *alarm*. Oleh karena itu, sistem dapat meningkatkan kepercayaan dan akuntabilitas operasional dengan membedakan secara lebih akurat serangan siber yang sebenarnya dari anomali yang disebabkan oleh kesalahan teknis atau kegagalan sensor.

Dalam pengembangan sistem berbasis kecerdasan buatan, metode kualitatif semakin penting. Mengacu pada paradigma data-centric *Explainable Artificial Intelligence* (XAI), transparansi model dipengaruhi oleh ketertelusuran dan integritas data masukan yang digunakan dalam proses pembelajaran [45].

Mekanisme ini selaras untuk implementasi keamanan perangkat keras, seperti penerapan teknologi *blockchain* di industri 4.0, yang dapat memastikan bahwa log keamanan sensor tetap utuh dan tidak dapat diubah selama proses mitigasi insiden berlangsung [51],[46].

Pendekatan *AI-Empowered* yang bersifat augmentatif (*AI-Augmented Architecture*) menegaskan bahwa peran *Explainable Artificial Intelligence* (XAI) bukan untuk menggantikan operator manusia, melainkan untuk memperkuat kemampuan analitik dalam memahami *log* jaringan fisik secara lebih komprehensif [41],[49].

3.7.5. Analisis Mendalam dan Implikasi Desain

Sebagian besar penelitian terdahulu berkonsentrasi pada pengembangan atau evaluasi algoritma tertentu, seperti Bi-LSTM atau CNN secara terpisah, tetapi rancangan konseptual H-ASICS menjawab masalah fragmentasi yang masih dominan dalam literatur saat ini. Metode ini tidak mempertimbangkan tingkat kompleksitas dan perbedaan ancaman siber yang dihadapi pada lingkungan operasional nyata.

Keunggulan adaptabilitas sistem yang disarankan dirancang untuk menjadi fleksibel terhadap perubahan karakteristik data karena menggunakan mekanisme Pembelajaran Mendalam Adaptatif (ADL). Struktur model dapat beradaptasi secara dinamis dengan tingkat kerumitan ancaman yang terdeteksi, meningkatkan atau menyederhanakan kompleksitasnya. Metode ini secara efektif mengatasi *trade-off* antara akurasi deteksi dan latensi pemrosesan, yang sering menjadi masalah penting dalam penelitian komputasi *edge* dan sistem waktu nyata.

4. Kesimpulan

Melalui *Sistematic Literature Review* (SLR) terhadap 51 penelitian terbaru (2022–2026), penelitian ini mengonfirmasi adanya pergeseran paradigma dalam keamanan siber infrastruktur kritis, transisi dari strategi pertahanan statis ke ekosistem cerdas yang adaptif. Temuan utama menunjukkan bahwa integrasi *Hybrid Deep Learning*, *Explainable Artificial Intelligence* (XAI), serta pemanfaatan pengetahuan domain fisik menjadi pendekatan yang paling menjanjikan dalam memitigasi ancaman kompleks seperti *False Data Injection* (FDI). Namun, masalah utama yang masih dihadapi termasuk keterbatasan efisiensi sumber daya pada perangkat *edge* dan kebutuhan untuk meningkatkan kepercayaan dalam operasional sistem dengan membuat model kecerdasan buatan transparan.

Sebagai kontribusi utama, penelitian ini mengusulkan kerangka kerja H-ASICS (*Hybrid Adaptive System for Infrastructure Critical Security*) yang mengadopsi model MAPE-K sebagai dasar pengelolaan sistem adaptif. H-ASICS menawarkan orkestrasi pertahanan melalui mesin seleksi algoritma adaptif yang mampu beralih secara dinamis antara *Hybrid* CNN-LSTM untuk pola temporal kompleks dan LightGBM untuk efisiensi komputasi rendah. Implementasi modul *Explainable Artificial Intelligence* (XAI), seperti SHAP dan LIME, yang dipadukan dengan teknologi blockchain dalam arsitektur ini berperan penting dalam menjamin akuntabilitas keputusan sistem serta menjaga integritas data log. Hal ini menjadi krusial dalam mendukung proses audit forensik pada lingkungan siber-fisik.

Arah penelitian di masa depan perlu difokuskan pada beberapa aspek strategis, yaitu validasi empiris arsitektur H-ASICS melalui implementasi pada *testbed* fisik berskala industri, pengembangan model *Deep Learning* yang lebih ringan (*lightweight*) agar dapat diimplementasikan secara optimal pada lingkungan *edge*, dan serta peningkatan ketahanan *adversarial* pada model AI guna menghadapi potensi serangan manipulatif terhadap sistem.

Secara keseluruhan, sinergi antara presisi deteksi, adaptabilitas operasional, dan transparansi keputusan menjadi fondasi utama dalam membangun sistem keamanan yang andal untuk melindungi infrastruktur kritis di masa depan.

Daftar Rujukan

[1] B. Pradevi, I. W. Wibisono, and R. O. Seba, "Kebijakan Pemerintahan Joko Widodo dalam Menghadapi Ancaman Cyber di Sektor Infrastruktur Energi Indonesia,"

SOSMANIORA (Jurnal Ilmu Sosial dan Humaniora), vol. 4, no. 3, pp. 908–917, Aug. 2025, doi: 10.55123/sosmaniora.v4i3.6424.

[2] J. J. Hidayat, A. P. Werdana, and C. Setyowati, "Perancangan Sistem Deteksi Gas dan Suhu Berbasis Mikrokontroler IoT Menggunakan Metode Prototyping," *Jurnal FASILKOM (teknologi inFormASi dan ILmu KOMputer)*, vol. 15, no. 2, pp. 398–407, 2025, doi: https://doi.org/10.37859/jf.v15i2.9173.

[3] J. P. A. Yaacoub, H. N. Noura, O. Salman, and K. Chahine, "Toward Secure Smart Grid Systems: Risks, Threats, Challenges, and Future Directions," *Future Internet*, vol. 17, no. 318, pp. 1–87, Jul. 2025, doi: 10.3390/fi17070318.

[4] D. R. Sari, "Analisis Keamanan Sistem Informasi dalam Era Internet of Things (IoT)," *Technologia Journal: Jurnal Informatika*, vol. 1, no. 2, pp. 1–10, 2024, doi: 10.62872/v2tffe44.

[5] M. T. Muslihi, "Pengembangan dan Evaluasi Sistem Monitoring Konsumsi Daya Listrik Berbasis IoT dengan Sensor PZEM-004T dan ESP8266," *Jurnal FASILKOM (teknologi inFormASi dan ILmu KOMputer)*, vol. 15, no. 1, pp. 77–83, 2025, doi: https://doi.org/10.37859/jf.v15i1.8508.

[6] D. Abraham, S. H. Houmb, and L. Erdodi, "Cyber-Attacks on Energy Infrastructure—A Literature Overview and Perspectives on the Current Situation," *Applied Sciences*, vol. 15, no. 17, pp. 1–19, Aug. 2025, doi: 10.3390/app15179233.

[7] Smart Idima, Philip Nwaga, and Patrick Evah, "Comprehensive Analysis of SCADA System Data for Intrusion Detection Using Machine Learning," *Global Journal of Engineering and Technology Advances*, vol. 22, no. 2, pp. 064–089, Feb. 2025, doi: 10.30574/gjeta.2025.22.2.0027.

[8] M. A. S. Arifin, Susanto, D. Stiawan, M. Y. Idris, and R. Budiarto, "The trends of supervisory control and data acquisition security challenges in heterogeneous networks," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 22, no. 2, pp. 874–883, Apr. 2021, doi: 10.11591/ijeecs.v22.i2.pp874-883.

[9] International Telecommunication Union (ITU), "Global Cybersecurity Index 2024," Geneva, 2024. Accessed: Dec. 16, 2025. [Online]. Available: https://www.itu.int/en/ITU-D/Cybersecurity/Documents/GCIv5/2401416_1b_Global-Cybersecurity-Index-E.pdf

[10] T. Nurhidayat *et al.*, *Kajian Ketahanan Siber: Manajemen Kerentanan*. Bogor, Indonesia: Politeknik Siber dan Sandi Negara, 2024. Accessed: Dec. 16, 2025. [Online]. Available: https://poltekssn.ac.id/wp-content/uploads/2024/12/101224_Buku_Kajian_Ketahanan_Keamanan_Siber_Manajemen_Kerentanan-1.pdf

[11] T. Yuliswar, I. Elfitri, and O. W. Purbo, "Optimization of Intrusion Detection System with Machine Learning for Detecting Distributed Attacks on Server," *Jurnal INOVTEK Polbeng - Seri Informatika*, vol. 10, no. 1, pp. 367–376, Mar. 2025, doi: 10.35314/vem9da98.

[12] K. Inayah and K. Ramli, "Analisis Kinerja Intrusion Detection System Berbasis Algoritma Random Forest Menggunakan Dataset Unbalanced Honeynet BSSN," *Jurnal Teknologi Informasi dan Ilmu Komputer (JTIIK)*, vol. 4, no. 11, pp. 867–876, Aug. 2024, doi: 10.25126/jtiik.1148911.

[13] A. Alsaiari and M. Ilyas, "A HYBRID CNN-LSTM DEEP LEARNING MODEL FOR INTRUSION DETECTION IN SMART GRID," *International Journal of Artificial Intelligence & Applications (IJAIA)*, vol. 16, no. 5, pp. 01–22, Sep. 2025, doi: 10.5121/ijaia.2025.16501.

[14] S. Ness, "Adversarial Attack Detection in Smart Grids Using Deep Learning Architectures," *IEEE Access*, vol. 13, pp. 16314–16323, 2025, doi: 10.1109/ACCESS.2024.3523409.

[15] A. Balla, M. H. Habaebi, M. R. Islam, and S. Mubarak, "Applications of deep learning algorithms for Supervisory Control and Data Acquisition intrusion detection system," Jul. 2022, *Elsevier Ltd*. doi: 10.1016/j.clet.2022.100532.

[16] B. Kitchenham and S. M. Charter, "Guidelines for performing Systematic Literature Reviews in Software Engineering," Durham, UK, 2007.

[17] X. J. Li, M. Ma, and Y. Sun, "An Adaptive Deep Learning Neural Network Model to Enhance Machine-Learning-Based Classifiers for Intrusion Detection in Smart Grids," *Algorithms*, vol. 16, no. 6, Jun. 2023, doi: 10.3390/a16060288.

[18] S. Y. Diaba *et al.*, "SCADA securing system using deep learning to prevent cyber infiltration," *Neural Networks*, vol. 165, pp. 321–332, Aug. 2023, doi: 10.1016/j.neunet.2023.05.047.

[19] P. Kumar, R. Kumar, A. Aljuhani, D. Javeed, A. Jolfaei, and A. K. M. N. Islam, "Digital twin-driven SDN for smart grid: A deep learning integrated blockchain for cybersecurity," *Solar Energy*, vol. 263, Aug. 2023, doi: 10.1016/j.solener.2023.111921.

[20] Y. Duan and Y. Zhang, "Enhancing smart grid security: A novel approach for efficient attack detection using SMART framework," *Measurement: Sensors*, vol. 32, Jan. 2024, doi: 10.1016/j.measen.2023.101015.

[21] F. Mesadieu, D. Torre, and A. Chennameneni, "Leveraging Deep Reinforcement Learning Technique for Intrusion Detection in SCADA Infrastructure," *IEEE Access*, vol. 12, pp. 63381–63399, 2024, doi: 10.1109/ACCESS.2024.3390722.

[22] S. Ness, "Adversarial Attack Detection in Smart Grids Using Deep Learning Architectures," *IEEE Access*, vol. 13, pp. 16314–16323, Jan. 2025, doi: 10.1109/ACCESS.2024.3523409.

[23] J. E. Efiong, J. E. T. Akinsola, B. O. Akinyemi, E. A. Olajubu, and G. A. Aderounmu, "A contrived dataset of substation automation for cybersecurity research in the smart grid networks based on IEC61850," *Telkomnika (Telecommunication Computing Electronics and Control)*, vol. 22, no. 5, pp. 1320–1330, Oct. 2024, doi: 10.12928/TELKOMNIKA.v22i5.26000.

[24] D. T. Ha, N. X. Hoang, N. V. Hoang, N. H. Du, T. T. Huong, and K. P. Tran, "Explainable Anomaly Detection for Industrial Control System Cybersecurity," in *IFAC-PapersOnLine*, Elsevier B.V., 2022, pp. 1183–1188. doi: 10.1016/j.ifacol.2022.09.550.

[25] P. Patel and A. P. Salave, "AI-Driven Cybersecurity Framework for Next-Gen Computing Applications and Critical Infrastructure," *Communications, and Computing Summit*, vol. 1, no. 1, pp. 1–10, Dec. 2023, [Online]. Available: https://doi.org/10.17051/ECC/01.01.01

[26] S. Idima, P. Nwaga, and P. Evah, "Comprehensive Analysis of SCADA System Data for Intrusion Detection Using Machine Learning," *Global Journal of Engineering and Technology Advances*, vol. 22, no. 2, pp. 064–089, Feb. 2025, doi: 10.30574/gjeta.2025.22.2.0027.

[27] R. Ithaya, R. Shobana, A. K. Mishra, and J. B. Christinal, "CAD-IGMS: Cyber attack detection in an intelligent grid management system via the deep learning enhancing grid reliability," *Ain Shams Engineering Journal*, vol. 16, no. 12, pp. 1–12, Oct. 2025, doi: 10.1016/j.asej.2025.103678.

[28] S. Kabir, N. Hannan, A. Shufian, and M. S. R. Zishan, "Proactive detection of cyber-physical grid attacks: A pre-attack phase identification and analysis using anomaly-based machine learning models," *Array*, vol. 27, pp. 1–18, Jun. 2025, doi: 10.1016/j.array.2025.100441.

[29] R. Bhukya, S. A. Moeed, A. Medavaka, A. O. Khadidos, A. O. Khadidos, and S. Selvarajan, "SPARK and SAD: Leading-edge deep learning frameworks for robust and effective intrusion detection in SCADA systems," *International Journal of Critical Infrastructure Protection*, vol. 49, pp. 1–24, Mar. 2025, doi: 10.1016/j.ijcip.2025.100759.

[30] A. O. Khadidos, A. O. Khadidos, S. Selvarajan, T. Al-Shehari, N. A. Alsadhan, and S. Singh, "CyberSentry: Enhancing SCADA security through advanced deep learning and optimization strategies," *International Journal of Critical Infrastructure Protection*, vol. 50, pp. 1–23, Jun. 2025, doi: 10.1016/j.ijcip.2025.100782.

[31] M. A. A. Sarker, B. Shanmugam, S. Azam, and S. Thennadil, "Enhancing smart grid load forecasting: An attention-based deep learning model integrated with federated learning and XAI for security and interpretability,"

P-ISSN : 2089-3353
E-ISSN : 2808-9162

Intelligent Systems with Applications, vol. 23, pp. 1–17, Aug. 2024, doi: 10.1016/j.iswa.2024.200422.

[32] Z. Zhang *et al.*, "A survey on resilient microgrid system from cybersecurity perspective," *Appl. Soft Comput.*, vol. 175, pp. 1–18, Apr. 2025, doi: 10.1016/j.asoc.2025.113088.

[33] K. S. Rao *et al.*, "Unveiling CyberFortis: A Unified Security Framework for IIoT-SCADA Systems with SiamDQN-AE FusionNet and PopHydra Optimizer," *Computers, Materials and Continua*, vol. 85, no. 1, pp. 1899–1916, Aug. 2025, doi: 10.32604/cmc.2025.064728.

[34] E. Altamimi, A. Al-Ali, A. K. Al-Ali, and Q. M. Malluhi, "Distribution-based residual analysis of load forecasting for enhanced anomaly detection," *International Journal of Electrical Power and Energy Systems*, vol. 173, pp. 1–13, Dec. 2025, doi: 10.1016/j.ijepes.2025.111435.

[35] M. Alanazi, A. Mahmood, and M. J. M. Chowdhury, "ICS-LTU2022: A dataset for ICS vulnerabilities," *Comput. Secur.*, vol. 148, pp. 1–28, Oct. 2024, doi: 10.1016/j.cose.2024.104143.

[36] S. A. Oyedotun, G. P. Oise, and C. E. Ozobialu, "Towards Intelligent Cybersecurity in SCADA and DCS Environments: Anomaly Detection Using Multimodal Deep Learning and Explainable AI," *Journal of Science Research and Reviews*, vol. 2, no. 3, pp. 20–31, Jul. 2025, doi: 10.70882/josrar.2025.v2i3.76.

[37] G. Aldehim, S. Basheer, A. S. Alluhaidan, and S. Sakri, "Robust False Data Injection Identification Framework for Power Systems Using Explainable Deep Learning," *Computers, Materials and Continua*, vol. 85, no. 2, pp. 3599–3619, Sep. 2025, doi: 10.32604/cmc.2025.065643.

[38] D. F. Valderrama *et al.*, "An online intrusion detection system for photovoltaic generators through physics-based neural networks," *Electric Power Systems Research*, vol. 253, pp. 1–9, Dec. 2025, doi: 10.1016/j.epsr.2025.112528.

[39] M. M. Pranav, R. S., R. D. A. Raj, A. Pallakonda, R. M. R. Yanamala, and K. P. K., "Smart grid cybersecurity against power system MiTM threats and machine learning-based attack classification," *Energy Reports*, vol. 15, pp. 1–23, Jan. 2026, doi: 10.1016/j.egyr.2025.12.035.

[40] X. Sun *et al.*, "A Hierarchical Federated Learning-Based Intrusion Detection System for 5G Smart Grids," *Electronics (Basel).*, vol. 11, no. 16, p. 2627, 2022, doi: 10.3390/electronics11162627.

[41] A. Kumari *et al.*, "AI-Empowered Attack Detection and Prevention Scheme for Smart Grid System," *Mathematics*, vol. 10, no. 16, p. 2852, 2022, doi: 10.3390/math10162852.

[42] N. Tariq, A. Alsirhani, M. Humayun, F. Alserhani, and M. Shaheen, "A fog-edge-enabled intrusion detection system for smart grids," *Journal of Cloud Computing*, vol. 13, no. 43, 2024, doi: 10.1186/s13677-024-00609-9.

[43] A. R. Singh *et al.*, "AI-enhanced smart grid framework for intrusion detection and mitigation in EV charging stations," *Alexandria Engineering Journal*, vol. 115, pp. 603–621, 2025, doi: 10.1016/j.aej.2024.12.061.

[44] R. Shrestha *et al.*, "Anomaly detection based on LSTM and autoencoders using federated learning in smart electric grid," *J. Parallel Distrib. Comput.*, vol. 193, pp. 1–13, 2024, doi: 10.1016/j.jpdc.2024.104951.

[45] R. Trivedi, S. Patra, and S. Khadem, "Data-centric explainable artificial intelligence techniques for cyber-attack detection in microgrid networks," *Energy Reports*, vol. 13, pp. 217–229, 2025, doi: 10.1016/j.egyr.2024.11.075.

[46] M. Barbhaya, P. R. Dasari, S. K. Damarla, R. Srinivasan, and B. Huang, "A deep learning framework for cyberattack detection and classification in Industrial Control Systems," *Comput. Chem. Eng.*, vol. 202, pp. 1–16, Nov. 2025, doi: 10.1016/j.compchemeng.2025.109278.

[47] U. Islam, H. Ullah, N. Khan, K. Saleem, and I. Ahmad, "AI-enhanced intrusion detection in smart renewable energy grids: A novel industry 4.0 cyber threat management approach," *International Journal of Critical Infrastructure Protection*, vol. 50, no. 1, pp. 1–16, 2025, doi: 10.1016/j.ijcip.2025.100769.

[48] M. Ammar, N. Javaid, A. K. J. Saudagar, and I. Ahmed, "An optimized Deep and Active Learning oriented framework for intrusion detection in Internet of Sensor Things," *Ain Shams Engineering Journal*, vol. 16, pp. 1–28, 2025, doi: 10.1016/j.asej.2025.103607.

[49] A. Sharma, S. Rani, and M. Shabaz, "Artificial intelligence-augmented smart grid architecture for cyber intrusion detection and mitigation in electric vehicle charging infrastructure," *Sci. Rep.*, vol. 15, no. 1, pp. 1–19, Dec. 2025, doi: 10.1038/s41598-025-04984-4.

[50] W. Ishtiaq, A. Zannat, A. H. M. S. Parvez, M. A. Hossain, M. H. Kanchan, and M. M. Tarek, "CST-AFNet: A dual attention-based deep learning framework for intrusion detection in IoT networks," *Array*, vol. 27, pp. 1–9, 2025, doi: 10.1016/j.array.2025.100501.

[51] A. Mahboob, M. Rashad, G. Abbas, Z. Mushtaq, T. Mazhar, and A. U. Rehman, "Fortifying Industry 4.0 Solar Power Systems: A Blockchain-Driven Cybersecurity Framework with Immutable LightGBM," *Computers, Materials and Continua*, vol. 85, no. 2, pp. 3805–3823, 2025, doi: 10.32604/cmc.2025.067615.

[52] A. Alsirhani, N. Tariq, M. Humayun, G. Naif Alwakid, and H. Sanaullah, "Intrusion detection in smart grids using artificial intelligence-based ensemble modelling," *Cluster Comput.*, vol. 28, no. 4, pp. 1–22, 2025, doi: 10.1007/s10586-024-04964-9.

[53] A. Villafranca and M.-D. Cano, "A hybrid inference pipeline for IDS: Combining DNNs and XGBoost through stacking for real-world intrusion detection," *Ad Hoc Networks*, vol. 188, p. 104227, 2026, doi: 10.1016/j.adhoc.2026.104227.

[54] A. Salehiyan, N. Serrano, F. Hernando-Gallego, D. Martín, and J. V. Álvarez-Bravo, "A Novel Evolutionary Optimized Transformer-Deep Reinforcement Learning Framework for False Data Injection Detection in Industry 4.0 Smart Water Infrastructures," *Computers, Materials and Continua*, vol. 87, no. 2, p. 68, 2026, doi: 10.32604/cmc.2026.075336.

[55] J. H. Kim, K. S. Son, J. G. Song, Y. G. Lee, and Y. J. Lee, "A study on process information-driven cyber threat detection for I&C systems in NPP," *Nuclear Engineering and Technology*, vol. 58, no. 1, p. 103879, 2026, doi: 10.1016/j.net.2025.103879.

[56] J. He, Y. Zheng, S. Lei, F. Liao, and L. Wu, "Cyber–physical intrusion detection for coordinated renewable energy and storage systems," *Array*, vol. 30, p. 100765, 2026, doi: 10.1016/j.array.2026.100765.

[57] N. M, A. N. V, B. S. P, and B. S, "Decentralized cybersecurity in smart grids: Leveraging location-fedavg for rapid threat detection and adaptive resilience," *Results in Engineering*, vol. 29, p. 108518, 2026, doi: 10.1016/j.rineng.2025.108518.

[58] H. Su, X. Zhang, L. Zheng, X. Shen, and H. Liao, "Deep Feature-Driven Hybrid Temporal Learning and Instance-Based Classification for DDoS Detection in Industrial Control Networks," *Computers, Materials and Continua*, vol. 86, no. 3, pp. 1–26, 2026, doi: 10.32604/cmc.2025.072093.

[59] D. Javaheri, H. Chizari, M. Fahmideh, M. H. Nadimi-Shahraki, and J. Hur, "DeepRadar: A cyber-defence interceptor for early warning and defusing malware injection attacks," *Knowl. Based. Syst.*, vol. 331, 2026, doi: 10.1016/j.knosys.2025.114830.

[60] M. S. Harish, S. Lokesh, P. Sakthivel, and B. Akshaya, "Hybrid deep learning model for network intrusion detection using optimal feature fusion," *Ain Shams Engineering Journal*, vol. 17, no. 1, pp. 1–29, 2026, doi: 10.1016/j.asej.2025.103904.

[61] S. H. Mohammed *et al.*, "IG-APSO-DNN: Deep learning intrusion detection model to detect false data injection attacks in smart grids," *Ad Hoc Networks*, vol. 180, pp. 1–14, 2026, doi: 10.1016/j.adhoc.2025.104053.

[62] H. Moayyed *et al.*, "Innovative defense strategies: Fusion deep learning approach to counter false data injection attacks in power systems," *Reliab. Eng. Syst. Saf.*, vol. 268, pp. 1–19, 2026, doi: 10.1016/j.ress.2025.112003.

[63] O. B. J. Rabie, S. Selvarajan, D. Alghazzawi, A. Kumar, S. Hasan, and M. Z. Asghar, "A security model for smart grid SCADA systems using stochastic neural network," *IET Generation, Transmission and Distribution*, vol. 17, no. 20, pp. 4541–4553, 2023, doi: 10.1049/gtd2.12943.

P-ISSN : 2089-3353
E-ISSN : 2808-9162

[64] H. Naeem, F. Ullah, and G. Srivastava, "Classification of intrusion cyber-attacks in smart power grids using deep ensemble learning with metaheuristic-based optimization," *Expert Syst.*, vol. 42, no. 1, 2025, doi: 10.1111/exsy.13556.