Jurnal Pendidikan dan Teknologi Indonesia (JPTI)
Vol. 5, No. 8, Agustus 2025, Hal. 2387-2401
DOI: https://doi.org/10.52436/1.jpti.954
p-ISSN: 2775-4227
e-ISSN: 2775-4219

Review Artikel : Studi Komprehensif Kinerja Sistem Keamanan Jaringan dalam Menangkal Serangan terhadap Infrastruktur Energi Listrik

Lendra Nur Aprilla[1], Ruki Harwahyu*[2]

[1,2]Departemen Teknik Elektro, Universitas Indonesia, Indonesia
Email: [1]lendra.nur@ui.ac.id, [2]ruki.h@ui.ac.id

Abstrak

Infrastruktur energi listrik semakin bergantung pada teknologi informasi dan komunikasi sehingga menjadi lebih rentan terhadap serangan siber. Ketergantungan ini menambah risiko serius terhadap keandalan dan keamanan sistem tenaga listrik, terutama dalam menghadapi serangan yang semakin canggih dan terorganisir. Penelitian ini bertujuan untuk mengevaluasi kinerja sistem keamanan jaringan dalam melindungi infrastruktur energi listrik dari ancaman siber. Metode yang digunakan adalah studi literatur dengan pendekatan analisis deskriptif terhadap berbagai teknik pertahanan yang telah diterapkan maupun yang sedang dikembangkan. Hasil kajian menunjukkan bahwa sistem deteksi intrusi (IDS), firewall cerdas, dan algoritma pembelajaran mesin adalah pendekatan yang paling umum dan efektif. Namun, beberapa kelemahan ditemukan, seperti keterbatasan dalam mendeteksi serangan zero-day, kurangnya kemampuan adaptasi terhadap pola serangan baru, serta integrasi sistem yang belum optimal. Berdasarkan temuan ini, penelitian ini merekomendasikan peningkatan integrasi teknologi berbasis kecerdasan buatan, penguatan respons waktu nyata (real-time response), dan perbaikan koordinasi antar sistem keamanan. Temuan ini diharapkan dapat menjadi dasar dalam pengembangan strategi keamanan siber yang lebih kuat dan adaptif untuk menjaga keandalan serta ketahanan infrastruktur energi listrik dalam jangka panjang.

Kata kunci: *Ancaman Siber, Keamanan infrastruktur, Keamanan Siber, Mekanisme pertahanan, SCADA, Sistem Tenaga Modern, Smart Grid.*

A Review Article : A Comprehensive Study of Network Security System Performance in Counteracting Attacks on Electric Power Infrastructure

Abstract

The electrical energy infrastructure is increasingly reliant on information and communication technology, making it more vulnerable to cyberattacks. This dependency adds significant risks to the reliability and security of power systems, particularly in the face of increasingly sophisticated and organized threats. This study aims to evaluate the performance of network security systems in protecting energy infrastructure from cyber threats. The method used is a literature review with a descriptive analysis approach of various defense techniques that have been implemented or are currently being developed.The results of the study indicate that intrusion detection systems (IDS), intelligent firewalls, and machine learning algorithms are among the most common and effective approaches. However, several weaknesses were identified, including limitations in detecting zero-day attacks, a lack of adaptability to new attack patterns, and suboptimal system integration. Based on these findings, this research recommends enhancing the integration of artificial intelligence-based technologies, strengthening real-time response capabilities, and improving coordination among security systems. These findings are expected to serve as a foundation for the development of stronger and more adaptive cybersecurity strategies to ensure the long-term reliability and resilience of electrical energy infrastructure.

Keywords: *Cyber Threat, Infrastructure security, Cyber Security, Defense mechanisms, SCADA, Modern Power Systems, Smart Grid.*

1. PENDAHULUAN

Infrastruktur energi listrik merupakan elemen penting dalam menjaga stabilitas ekonomi dan kesejahteraan masyarakat. Seiring meningkatnya kebutuhan energi dan pemanfaatan sumber daya terbarukan, sistem tenaga listrik menghadapi tekanan untuk menjadi lebih efisien, fleksibel, dan berkelanjutan. Transformasi ini mendorong pengembangan *smart grid*, yaitu jaringan listrik cerdas yang mengintegrasikan teknologi informasi dan komunikasi (TIK) untuk memungkinkan pengelolaan energi secara otomatis, real-time, dan dua arah [14][18].

p-ISSN: 2775-4227
e-ISSN: 2775-4219

Namun, digitalisasi sistem ini juga menimbulkan tantangan serius berupa meningkatnya risiko serangan siber terhadap jaringan listrik dan komponen kritis seperti sistem SCADA (Supervisory Control and Data Acquisition). Ketergantungan pada sistem digital membuka peluang bagi aktor jahat untuk meluncurkan serangan yang berpotensi menyebabkan gangguan operasional besar, pemadaman listrik, bahkan ancaman terhadap keamanan nasional [2]. Keamanan siber dalam sistem tenaga listrik modern yang semakin terdigitalisasi dan terhubung melalui berbagai komponen seperti pembangkit, transmisi, dan distribusi [1]. Ancaman serangan siber merupakan salah satu prioritas tertinggi dalam spektrum ancaman terhadap keamanan nasional, seiring berkembangnya bentuk konflik dari tradisional menjadi *hybrid warfare* (gabungan fisik dan digital) [9]. Pentingnya melindungi sistem energi terbarukan dari ancaman serangan siber dan pelanggaran data, yang semakin relevan karena meningkatnya ketergantungan pada teknologi digital dan sistem yang terhubung [15]. Ancaman siber yang terus berkembang, seperti sabotase, penipuan, dan kebocoran data, dapat memiliki dampak yang sangat merugikan bagi perusahaan, konsumen, dan bahkan negara secara keseluruhan [13]. Keamanan siber menjadi sangat penting untuk mencegah serangan yang dapat mengganggu pasokan energi dan berisiko terhadap keamanan nasional [12].

Berbagai studi sebelumnya menunjukkan bahwa sistem energi, terutama yang menggunakan teknologi OT (Operational Technology), rentan terhadap serangan seperti *False Data Injection (FDI)*, *Denial of Service (DoS)*, *Man-in-the-Middle (MITM)*, hingga *ransomware* [16]. Kasus-kasus seperti serangan terhadap jaringan listrik Ukraina (2015), penyebaran malware Stuxnet (2010), dan insiden SolarWinds (2020) menjadi bukti nyata tingginya eskalasi serangan terhadap sektor energi [7][8][3]. Di Indonesia pernah terjadi serangan ransomware WannaCry pada 2017 berdampak pada sistem rumah sakit, sementara gangguan listrik besar-besaran di Jabodetabek pada 2019 mengindikasikan pentingnya kesiapan infrastruktur, meskipun penyebabnya bukan serangan langsung [5]. Strategi pertahanan konvensional seperti firewall, enkripsi, dan kontrol akses telah diterapkan, namun terbukti memiliki keterbatasan terhadap serangan yang semakin canggih. Oleh karena itu, pendekatan yang lebih adaptif seperti *Moving Target Defense (MTD)*, *Quantum Key Distribution (QKD)*, model *Zero Trust*, dan teknologi pembelajaran mesin mulai banyak diteliti dan dikembangkan untuk memperkuat ketahanan system [6][11] .

Tulisan ini bertujuan untuk meninjau dan mengevaluasi kinerja sistem keamanan jaringan dalam menangkal serangan terhadap infrastruktur energi listrik. Kajian ini difokuskan pada identifikasi jenis-jenis ancaman yang umum terjadi, analisis terhadap efektivitas teknik pertahanan yang ada, serta eksplorasi terhadap solusi inovatif yang dapat diterapkan untuk meningkatkan postur keamanan siber sektor energi. Melalui pendekatan studi literatur, artikel ini diharapkan dapat memberikan kontribusi dalam penyusunan strategi keamanan yang lebih tangguh dan adaptif di era digital.

2. METODE PENELITIAN

Penelitian ini menggunakan studi literatur sebagai metode pengumpulan data. Studi literatur ini berfungsi untuk mengumpulkan informasi dari berbagai sumber yang relevan dengan topik penelitian,yang membahas tentang keamanan siber dalam sistem tenaga listrik, terutama pada infrastruktur yang menghubungkan pembangkit, transmisi, dan distribusi tenaga listrik.

2.1. Desain Penelitian

Penelitian ini merupakan studi literatur dengan pendekatan analisis deskriptif. Tujuan dari penelitian ini adalah untuk mengidentifikasi dan menjelaskan berbagai ancaman siber yang dapat memengaruhi sistem tenaga listrik yang terhubung secara digital. Setelah pengumpulan data, dilakukan analisis deskriptif untuk menguraikan informasi yang diperoleh dari sumber-sumber yang relevan, serta menjelaskan implikasi dari temuan tersebut terhadap keamanan sistem tenaga listrik.

2.2. Sumber Data

Sumber data dalam penelitian ini melibatkan jurnal nasional dan internasional yang relevan, mencakup hal-hal berikut:

- Pembahasan terkait keamanan siber, infrastruktur energi, dan sistem tenaga listrik.
- Sumber yang terpercaya yang mengulas teknologi terbaru serta ancaman siber terhadap smart grid dan sistem SCADA.
- Penjelasan mengenai teori dasar sistem tenaga listrik dan infrastruktur komunikasi yang digunakan dalam sistem distribusi energi.

p-ISSN: 2775-4227
e-ISSN: 2775-4219

2.3. Prosedur Pengumpulan Data

Proses pengumpulan data dilakukan melalui beberapa tahapan:

1. Pencarian data: Data diperoleh melalui pencarian literatur di database ilmiah seperti Google Scholar, IEEE Xplore, dan lainnya.
2. Seleksi data: Artikel yang dipilih harus relevan dengan topik yang dibahas, mencakup pendekatan teknologi keamanan dalam sistem tenaga listrik, serta masalah dan solusi terkait ancaman siber dalam sistem SCADA, smart grid, dan energi terbarukan.
3. Pengambilan data: Artikel yang memenuhi kriteria dipelajari secara mendalam untuk mendapatkan informasi yang dibutuhkan dalam penelitian ini.

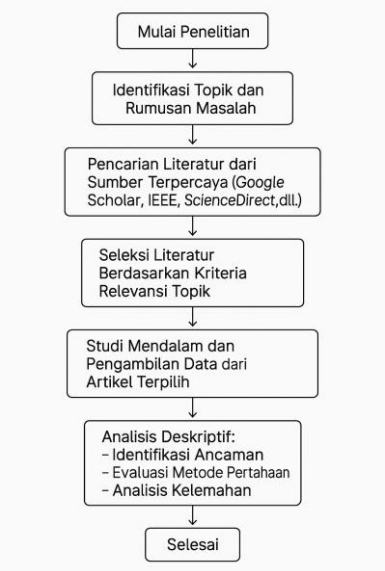
2.4. Teknik Analisis Data

Data yang terkumpul dianalisis menggunakan pendekatan klasifikasi metode keamanan yang ada dalam literatur. Proses analisis meliputi:

1. Identifikasi ancaman siber: Meneliti dan mengklasifikasikan jenis-jenis serangan siber yang dapat memengaruhi sistem tenaga listrik, seperti Distributed Denial of Service (DDoS), malware pada sistem SCADA, False Data Injection Attack (FDIA), dan serangan koordinasi siber-fisik.
2. Evaluasi teknik pertahanan: Mengkaji efektivitas berbagai metode pertahanan yang ada, termasuk penggunaan enkripsi, autentikasi, serta penerapan teknologi baru seperti kecerdasan buatan dan jaringan saraf tiruan untuk deteksi dan mitigasi ancaman.
3. Analisis celah keamanan: Mengidentifikasi celah atau kelemahan dalam protokol komunikasi yang dapat dimanfaatkan oleh ancaman siber, serta mengusulkan langkah-langkah mitigasi yang dapat diterapkan.

2.5. Diagram Alur Metode Penelitian

Untuk memperjelas tahapan analisis, berikut adalah diagram alur yang menggambarkan langkah-langkah dalam metode penelitian ini:



Gambar 1. Diagram Alur Metode Penelitian

Dengan mengikuti metode yang telah dijelaskan, penelitian ini bertujuan untuk memberikan gambaran yang jelas mengenai ancaman siber dalam sistem tenaga listrik serta solusi yang dapat diterapkan untuk memperkuat keamanannya.

Dengan demikian, penelitian ini menyajikan berbagai pendekatan dalam mengamankan infrastruktur energi dari ancaman siber.

p-ISSN: 2775-4227
e-ISSN: 2775-4219

3. HASIL DAN PEMBAHASAN

3.1. Hasil

Studi literatur ini memberikan analisis mendalam mengenai berbagai pendekatan keamanan siber yang diterapkan pada sistem tenaga listrik modern, khususnya pada Supervisory Control and Data Acquisition (SCADA), smart grid, dan Cyber-Physical Power Systems (CPPS). Berdasarkan hasil simulasi, studi kasus, dan model analitik, penelitian ini mengidentifikasi kekuatan serta kelemahan dari berbagai metode yang diterapkan.

- Sistem SCADA dan Kerentanannya

  Sistem SCADA, yang banyak digunakan untuk pengelolaan infrastruktur tenaga, terbukti memiliki kelemahan signifikan pada protokol komunikasinya, seperti Modbus dan DNP3 [39]. Meskipun masih digunakan secara luas, protokol ini tidak dirancang untuk menghadapi ancaman siber modern karena tidak adanya fitur enkripsi dan autentikasi internal. Simulasi menunjukkan bahwa sistem ini sangat rentan terhadap serangan seperti Denial of Service (DoS), Man-in-the-Middle (MitM), dan false data injection (FDI) [7].
- Deteksi dan Pencegahan Intrusi (IDS/IPS)

  Pendekatan deteksi dan pencegahan intrusi berbasis autentikasi byte unik dan algoritma enkripsi terbukti efektif dalam mengidentifikasi serangan konvensional serta mencegah penetrasi awal. Meskipun demikian, efektivitasnya berkurang terhadap serangan lanjutan yang lebih terkoordinasi, seperti serangan hybrid, karena keterbatasannya dalam beradaptasi dengan pola serangan baru [29].
- Penggunaan Teknologi Kecerdasan Buatan

  Teknologi kecerdasan buatan, terutama model Convolutional Neural Network (CNN) dan Long Short-Term Memory (LSTM), menunjukkan tingkat akurasi deteksi lebih dari 98% untuk serangan seperti replay attack, DoS, dan FDI. Model-model ini unggul dalam mengenali pola kompleks dan non-linier pada data operasional. Namun, keberhasilan metode ini sangat bergantung pada kualitas data pelatihan serta kebutuhan akan sumber daya komputasi yang besar [28].
- Blockchain dalam Smart Grid

  Teknologi blockchain dievaluasi sebagai solusi potensial untuk menjaga integritas dan transparansi data dalam sistem smart grid. Dengan sifat desentralisasi dan tidak dapat diubah (immutable), blockchain memberikan perlindungan terhadap manipulasi data dan pelanggaran privasi. Namun, tantangan yang dihadapi adalah keterbatasan skalabilitas dan latensi, yang menghambat penerapannya dalam sistem yang memerlukan respons waktu nyata [10].
- Ancaman Demand Load-Altering Attack–False Data Injection (DLAA-FDI)

  Serangan kombinasi antara manipulasi beban dan penyisipan data palsu, yang dikenal dengan Demand Load-Altering Attack–False Data Injection (DLAA-FDI), terbukti sangat berbahaya. Serangan ini dapat menyebabkan osilasi frekuensi dan ketidakstabilan sistem, terutama pada sistem yang memiliki penetrasi tinggi dari sumber energi terdistribusi (Distributed Energy Resources/DER). Hal ini menyoroti pentingnya integrasi antara keamanan siber dan kestabilan sistem fisik [26].
- Quantum Key Distribution (QKD)

  Quantum Key Distribution (QKD) dievaluasi sebagai pendekatan kriptografi generasi baru untuk meningkatkan tingkat keamanan dalam distribusi kunci. Meskipun potensi QKD dalam memberikan keamanan tinggi sangat menjanjikan, penerapannya masih terbatas oleh biaya implementasi yang tinggi dan tantangan dalam integrasi dengan sistem yang sudah ada [21].
- Kerentanan pada Cyber-Physical Power Systems (CPPS)

  Dalam konteks CPPS, kerentanannya terhadap serangan siber yang dapat memengaruhi baik sistem fisik maupun digital secara simultan masih sangat tinggi. Pendekatan seperti residual analysis dan Kalman filter terbukti efektif dalam mendeteksi dan mengoreksi sebagian besar anomali. Sistem deteksi berbasis deep learning bahkan menunjukkan performa unggul dalam menghadapi serangan yang lebih kompleks [32][34].
- Strategi Pertahanan Canggih

  Mengingat meningkatnya kompleksitas ancaman, berbagai strategi pertahanan canggih telah dikembangkan, seperti Moving Target Defense (MTD), pendekatan berbasis teori permainan (game theory), dan optimasi topologi jaringan. Strategi ini dirancang untuk memberikan pertahanan yang dinamis dan adaptif terhadap pola serangan yang terus berkembang [35].
- Pengembangan Testbed untuk Jaringan Transmisi Smart Grid

  Transformasi digital sistem tenaga listrik menuntut platform uji (*testbed*) yang mampu merepresentasikan kondisi operasional sebenarnya dalam smart grid. Testbed ini menggabungkan elemen fisik, virtual, dan emulasi dari komponen utama seperti gardu listrik, sistem SCADA, dan infrastruktur

p-ISSN: 2775-4227
e-ISSN: 2775-4219

komunikasi real-time. Tujuannya adalah untuk mengidentifikasi titik-titik kerentanan, menyediakan data empiris guna meningkatkan ketahanan siber, dan menjadi platform edukatif untuk pelatihan teknis dan eksperimen keamanan [19]. Kasus nyata seperti serangan siber terhadap infrastruktur energi di Ukraina (2015 dan 2021) menjadi pendorong utama pengembangan testbed. Studi seperti HINT-Sec telah memperluas model ini untuk pembangkit listrik tenaga nuklir melalui pendekatan *hardware-in-the-loop* (HIL) [30]. Pengembangan testbed semacam ini diharapkan menjadi standar baru dalam pengujian dan mitigasi risiko di sektor energi, sehingga disarankan untuk meningkatkan keamanan jaringan melalui penerapan sistem yang lebih andal, memanfaatkan testbed sebagai sarana pengujian berbagai skenario serangan, serta melakukan riset lanjutan guna mengembangkan strategi deteksi dan mitigasi yang lebih efektif [20].

- Simulasi Transien untuk Analisis Dampak Load-Altering Attack (LAA)

  Simulasi transien berbasis arus injeksi dikembangkan untuk menganalisis dampak Load-Altering Attack (LAA) pada sistem tenaga. Framework ini mencakup dua jenis serangan (ON/OFF dan umpan balik) serta respons sistem proteksi. Pengujian pada sistem IEEE 68-bus menunjukkan bahwa LAA dapat menyebabkan gangguan frekuensi serius hingga risiko pemadaman total [25].
- Interdependensi Siber-Fisik dalam Operasi Sistem Tenaga

  Ketergantungan antara aspek siber dan fisik dalam smart grid menciptakan dinamika baru yang kompleks. Dengan pendekatan *co-simulation* dan *digital twin*, studi internasional menunjukkan pentingnya memahami keterkaitan ini dalam membangun strategi pertahanan yang adaptif [23]. Pengembangan SDM melalui pelatihan dan pendidikan juga menjadi aspek krusial dalam membangun ketahanan sistem secara menyeluruh.

Secara keseluruhan, hasil penelitian ini menunjukkan bahwa meskipun ada berbagai pendekatan yang efektif dalam meningkatkan keamanan sistem tenaga listrik, tantangan besar masih ada terkait dengan skalabilitas, adaptasi terhadap serangan baru, dan integrasi teknologi yang lebih canggih.

3.2. Pembahasan

Secara keseluruhan, hasil studi ini memperkuat temuan-temuan dari penelitian sebelumnya mengenai pentingnya pendekatan berlapis dan integratif dalam menghadapi ancaman siber pada sistem tenaga listrik. Meskipun teknologi baru seperti AI dan blockchain memberikan solusi yang lebih efektif dibandingkan metode konvensional, tantangan terkait implementasi dan integrasi dalam sistem yang ada tetap harus diatasi. Oleh karena itu, pengembangan sistem keamanan yang tangguh memerlukan kombinasi berbagai teknologi, infrastruktur pengujian yang realistis, dan penguatan sumber daya manusia agar dapat beradaptasi dengan ancaman yang terus berkembang.

Salah satu aspek penting yang juga diperkuat oleh studi ini adalah urgensi keamanan sistem Cyber-Physical Systems (CPS) dalam smart grid. CPS merupakan sistem yang mengintegrasikan komponen fisik—seperti sensor dan aktuator—dengan jaringan siber untuk memantau dan mengendalikan berbagai proses di bidang-bidang penting seperti smart grid, perangkat medis, manufaktur, dan infrastruktur sipil. Sistem ini terdiri dari elemen-elemen utama seperti sensor, aktuator, serta jaringan komunikasi yang saling terhubung dan berinteraksi secara real-time [52]. Dengan semakin meluasnya penerapan CPS di berbagai sektor, kebutuhan akan sistem yang aman dan andal menjadi sangat krusial. Keamanan dalam CPS tidak dapat hanya bergantung pada kebijakan atau perlindungan di tingkat aplikasi, tetapi harus dirancang sejak tahap awal pengembangan sistem. Karena integrasi erat antara dunia fisik dan siber, kerentanan pada berbagai lapisan sistem—baik fisik, komunikasi, maupun kontrol—dapat dimanfaatkan oleh penyerang untuk mengganggu operasi dan stabilitas sistem tenaga secara keseluruhan. Serangan semacam ini tidak hanya berdampak pada data dan informasi, tetapi juga berpotensi menimbulkan kerusakan nyata pada infrastruktur fisik. Dalam konteks ini, penting untuk mengingat bahwa ancaman pada smart meter dapat berpotensi menyebabkan kebakaran jika tidak ditangani dengan baik, mengingat perangkat ini beroperasi dalam jaringan yang sangat terhubung dan dapat dipengaruhi oleh serangan siber [48]. Dengan sifat ancaman yang kompleks dan terus berkembang, tidak ada satu solusi tunggal yang mampu menjawab seluruh permasalahan keamanan yang ada. Oleh karena itu, penggabungan pendekatan keamanan fisik dan siber secara holistik menjadi elemen kunci dalam desain sistem smart grid yang aman, tangguh, dan adaptif terhadap berbagai skenario serangan [51].Smart grid menawarkan efisiensi tinggi dan integrasi yang lebih baik dengan sumber energi terbarukan dibandingkan jaringan listrik tradisional. Namun, sistem ini juga menghadapi tantangan serius, khususnya dalam hal keamanan siber dan privasi data. Salah satu ancaman utama adalah *False Data Injection Attack* (FDIA), yaitu serangan di mana data palsu disuntikkan ke sistem untuk mengganggu kinerjanya [17]. Untuk menghadapi risiko tersebut, sejumlah solusi telah diusulkan, seperti penerapan autentikasi dua faktor, peningkatan riset dan pelatihan di bidang keamanan, serta penguatan kebijakan untuk melindungi data pelanggan dan menjamin operasional yang aman [4]. Pendekatan-pendekatan ini penting karena tantangan keamanan tidak

p-ISSN: 2775-4227
e-ISSN: 2775-4219

hanya bersifat teknis, tetapi juga melibatkan aspek kebijakan serta kesadaran dan kapasitas sumber daya manusia yang terlibat. Smart grid berbasis IoT sangat rentan terhadap serangan karena tingginya kompleksitas sistem, banyaknya perangkat yang saling terhubung, serta ketergantungan pada komunikasi waktu nyata. Ancaman dalam sistem ini umumnya diklasifikasikan berdasarkan prinsip CIA (Confidentiality, Integrity, Availability), termasuk juga serangan tingkat lanjut. Untuk memperkuat pertahanan, teknologi mutakhir seperti kecerdasan buatan (AI), blockchain, dan *Software Defined Networking* (SDN) dinilai memiliki potensi besar dalam meningkatkan keamanan siber smart grid [27].

Dalam konteks ini, penting untuk memahami bahwa sistem tenaga listrik global sedang mengalami transformasi menuju Smart Grid. Smart Grid merupakan sistem cerdas yang mengintegrasikan tiga lapisan utama: energi/power, komunikasi, dan teknologi informasi (IT), untuk meningkatkan efisiensi, keamanan, dan keandalan distribusi listrik. Teknologi ini memungkinkan aliran energi dan informasi dua arah, serta mendukung penggunaan energi terbarukan, kontrol otomatis, dan keterlibatan konsumen dalam pengelolaan konsumsi energi. Smart Grid adalah masa depan sistem tenaga listrik, karena menggabungkan teknologi digital dan sensor pintar yang dapat meningkatkan efisiensi, keandalan, dan keamanan jaringan listrik. Sistem ini memiliki kemampuan pemantauan dan perbaikan mandiri (self-healing), sehingga dapat mendeteksi dan merespons gangguan secara otomatis, tanpa keterlibatan manual yang signifikan. Dibandingkan grid tradisional, Smart Grid menawarkan: distribusi daya dua arah, integrasi sumber energi terbarukan (seperti panel surya), pemantauan konsumsi energi secara real-time melalui smart meter dan sistem SCADA, serta pilihan yang lebih fleksibel bagi konsumen. Smart Grid mendukung efisiensi energi dan pengurangan biaya, serta berkontribusi pada pembangunan ekonomi dan keberlanjutan lingkungan. Dengan kemajuan teknologi informasi dan komunikasi (ICT), Smart Grid menjadi sistem yang adaptif, aman secara siber, dan berorientasi masa depan. Pemerintah dan lembaga energi harus mendorong adopsi Smart Grid secara nasional untuk mengurangi ketergantungan pada sistem listrik konvensional dan mendukung keberlanjutan energi. Penguatan sistem keamanan siber perlu diperhatikan untuk menjaga keandalan dan integritas data dalam jaringan listrik pintar [45].

Hasil studi ini menunjukkan bahwa sistem tenaga listrik modern, terutama yang menggunakan SCADA, masih rentan terhadap ancaman siber, seiring dengan digunakannya protokol komunikasi lama seperti Modbus dan DNP3 yang tidak memiliki mekanisme keamanan modern seperti autentikasi dan enkripsi. Hal ini serupa dengan temuan pada penelitian sebelumnya, yang menunjukkan bahwa protokol ini tidak dirancang untuk menghadapi ancaman yang lebih canggih dan berpotensi menempatkan sistem tenaga pada risiko serangan serius, seperti manipulasi data dan gangguan layanan (*Denial of Service*).

Sebagai respons terhadap berbagai kerentanan keamanan yang ada, baik penelitian terdahulu maupun studi ini sama-sama menekankan pentingnya adopsi teknologi mutakhir, seperti kecerdasan buatan (AI) dan blockchain, untuk memperkuat pertahanan sistem. Penelitian sebelumnya mengenai penerapan AI, khususnya dengan menggunakan model *deep learning* seperti *Convolutional Neural Network (CNN)* dan *Long Short-Term Memory (LSTM)*, menunjukkan bahwa model-model ini memiliki kemampuan mendeteksi serangan yang lebih kompleks dan dinamis. Serangan-serangan tersebut sering kali tidak terdeteksi oleh sistem deteksi dan pencegahan intrusi (IDS/IPS) tradisional yang berbasis signature. Temuan ini sejalan dengan hasil studi ini, yang menunjukkan bahwa model *deep learning* tidak hanya mampu mengenali pola serangan yang kompleks, tetapi juga efektif dalam mendeteksi serangan *zero-day* dan pola-pola non-linier yang sulit diidentifikasi dengan pendekatan konvensional. Dengan kata lain, penerapan AI tidak hanya meningkatkan akurasi dalam deteksi ancaman, tetapi juga memperluas kemampuan sistem untuk mengidentifikasi jenis serangan yang belum pernah dikenali sebelumnya [28].

Lebih lanjut, dalam konteks deteksi dan mitigasi ancaman siber pada *Cyber-Physical Production Systems (CPPS)*, studi ini juga mengidentifikasi sejumlah kelemahan dalam pendekatan yang telah ada. Salah satu temuan utama adalah efektivitas penggunaan *Deep Reinforcement Learning* berbasis *Graph Convolutional Network* untuk mendeteksi ancaman pada sistem energi transaktif. Pendekatan ini menawarkan peningkatan yang signifikan dalam aspek keamanan, akurasi, keandalan, dan skalabilitas dibandingkan metode-metode sebelumnya [37].

Di sisi lain, teknologi blockchain memberikan pendekatan yang berbeda untuk mengatasi masalah integritas data yang rentan terhadap manipulasi. Blockchain menawarkan sistem desentralisasi yang mencatat semua transaksi atau perubahan data dalam bentuk yang tidak dapat diubah (*immutable*). Penelitian sebelumnya telah menggarisbawahi keunggulan blockchain dalam menjaga transparansi dan integritas data pada sistem smart grid, yang mengandalkan komunikasi dua arah antar perangkat. Seperti yang ditunjukkan dalam studi ini, blockchain sangat relevan untuk mengurangi risiko manipulasi data oleh pihak ketiga yang tidak sah. Dibandingkan dengan enkripsi konvensional seperti AES yang hanya melindungi data selama transmisi, blockchain memberikan lapisan keamanan tambahan dengan menghilangkan ketergantungan pada otoritas pusat yang bisa menjadi titik kegagalan. Untuk itu, teknologi blockchain menawarkan pendekatan inovatif melalui prinsip desentralisasi, pencatatan transaksi yang tidak dapat diubah (*immutable ledger*), serta pengurangan ketergantungan pada pihak ketiga. Salah satu fitur unggulan blockchain dalam konteks smart grid adalah penerapan *smart contract*, yang memungkinkan otomatisasi transaksi energi secara langsung antara prosumer (produsen sekaligus konsumen energi) dan

p-ISSN: 2775-4227
e-ISSN: 2775-4219

konsumen tanpa perantara. Transaksi ini bersifat aman, dapat diaudit, dan berlangsung secara real-time, sehingga tidak hanya mempercepat proses distribusi energi, tetapi juga mengurangi biaya dalam skema *transactive energy* serta memperkuat privasi pengguna [46].

Namun, meskipun blockchain unggul dalam hal integritas dan transparansi, tantangan seperti latensi tinggi dan keterbatasan skalabilitas tetap menjadi hambatan, terutama untuk aplikasi yang memerlukan respons cepat dalam waktu nyata, seperti pengendalian beban dan stabilisasi frekuensi. Hal ini juga tercermin dalam penelitian sebelumnya yang mencatat bahwa penggunaan blockchain pada sistem yang memerlukan kecepatan transaksi tinggi, seperti dalam kontrol dinamis sistem tenaga, belum sepenuhnya optimal. Dengan demikian, meskipun blockchain menawarkan solusi yang lebih baik dibandingkan enkripsi tradisional dalam hal transparansi dan ketahanan terhadap manipulasi, penerapannya membutuhkan inovasi lebih lanjut untuk mengatasi kendala latensi dan skalabilitas.

Selain teknologi AI dan blockchain, penerapan *Cybersecurity Framework* dalam konteks *smart grid* juga sangat relevan. Framework ini membantu pemilik/operator sistem tenaga dalam memprioritaskan aktivitas keamanan siber yang mendukung keselamatan, keandalan, ketahanan, dan modernisasi jaringan. Dengan mengorganisasi aktivitas keamanan ke dalam lima fungsi inti—Identify, Protect, Detect, Respond, dan Recover—pendekatan ini tidak hanya menyediakan struktur dalam manajemen risiko, tetapi juga menekankan pentingnya manajemen risiko pihak ketiga dan rantai pasokan. Framework ini juga memberikan pertimbangan praktis untuk mengatasi tantangan keamanan dalam transformasi sistem tenaga listrik menuju era digital [38].

Quantum Key Distribution (QKD) sebagai metode kriptografi yang muncul sebagai solusi masa depan juga sejalan dengan penelitian terdahulu yang menunjukkan potensi besar dalam mengamankan komunikasi yang sangat sensitif. QKD menjamin bahwa intersepsi dalam komunikasi dapat terdeteksi secara langsung karena perubahan informasi kuantum tidak dapat terjadi tanpa meninggalkan jejak. Namun, biaya tinggi dan keterbatasan jangkauan operasional saat ini menjadi hambatan besar untuk penerapannya dalam skala yang lebih luas, seperti yang juga disoroti dalam penelitian sebelumnya. Ini menunjukkan bahwa meskipun QKD menawarkan keamanan yang sangat tinggi, pengembangannya dalam sistem tenaga listrik memerlukan waktu dan investasi yang cukup besar.

Lebih lanjut, serangan yang semakin kompleks seperti *hybrid DLAA-FDI* menunjukkan tantangan ganda dalam sistem tenaga listrik, yaitu gangguan pada kestabilan fisik sistem serta penyusupan data yang tampak sah [26]. Penelitian sebelumnya juga menunjukkan bahwa serangan seperti ini memerlukan pendekatan pertahanan yang dapat menangani kedua aspek ini secara bersamaan. Dalam hal ini, hasil studi ini konsisten dengan literatur sebelumnya yang menekankan pentingnya menggabungkan teknologi seperti AI, blockchain, dan sistem kontrol adaptif untuk menciptakan sistem pertahanan yang lebih holistik. Terlebih lagi, teknik seperti *residual analysis* dan *Kalman filter* dapat mendeteksi anomali sederhana, tetapi serangan yang lebih kompleks memerlukan pendekatan *hybrid* berbasis AI, seperti *Graph Convolutional Networks (GCN)* dan *Deep Reinforcement Learning (DRL)*, yang menunjukkan kemajuan dalam menghadapi dinamika sistem energi yang semakin rumit [34].

Strategi pertahanan adaptif seperti *Moving Target Defense (MTD)* dan *game theory* telah terbukti efektif dalam beberapa studi sebelumnya sebagai solusi untuk menghadapi serangan yang terus berkembang. Hal ini juga tercermin dalam studi ini, yang menunjukkan bahwa kedua pendekatan ini memungkinkan sistem untuk secara dinamis mengubah konfigurasi keamanannya atau mengantisipasi strategi penyerang, meningkatkan ketahanan sistem terhadap ancaman yang tidak dapat diprediksi. Strategi-strategi ini memberikan fleksibilitas dan ketahanan lebih, namun mereka juga memperkenalkan kompleksitas dalam implementasi dan membutuhkan sumber daya yang besar untuk pengelolaannya [22].

Selain itu, inovasi dalam pengendalian sistem juga diperlukan. Salah satunya adalah pengembangan kontrol frekuensi berbasis *cyber-resilient*, yang tetap menjaga stabilitas sistem meskipun terjadi serangan atau gangguan komunikasi [33]. Penelitian terbaru dengan pendekatan *Lyapunov–Krasovskii* membuktikan bahwa sistem pengendalian dapat tetap stabil meski mengalami *delay* komunikasi atau injeksi data palsu [31].

Secara keseluruhan, hasil studi ini memperkuat temuan-temuan dari penelitian sebelumnya mengenai pentingnya pendekatan berlapis dan integratif dalam menghadapi ancaman siber pada sistem tenaga listrik. Meskipun teknologi baru seperti AI dan blockchain memberikan solusi yang lebih efektif dibandingkan metode konvensional, tantangan terkait implementasi dan integrasi dalam sistem yang ada tetap harus diatasi. Oleh karena itu, pengembangan sistem keamanan yang tangguh memerlukan kombinasi berbagai teknologi, infrastruktur, serta kerangka kerja yang adaptif dan terintegrasi untuk menghadapi ancaman siber yang terus berkembang di era digital.

3.6. Tabel Hasil, Perbedaan, dan Perbandingan Sistem Tenaga

Untuk memperoleh pemahaman yang komprehensif mengenai pendekatan keamanan siber dalam sistem tenaga modern, dilakukan perbandingan berdasarkan studi literatur dari berbagai sumber. Tabel berikut

p-ISSN: 2775-4227
e-ISSN: 2775-4219

merangkum topik-topik utama yang dibahas, mulai dari isu teknis seperti kelemahan protokol SCADA hingga teknologi mutakhir seperti Quantum Key Distribution (QKD) dan penggunaan artificial intelligence dalam deteksi ancaman.

Analisis ini disusun guna mengidentifikasi pola umum, membedakan pendekatan yang digunakan pada masing-masing teknologi, serta mengevaluasi efektivitas metode keamanan berdasarkan hasil dan temuan yang dilaporkan. Perbandingan ini juga menjadi dasar dalam menyusun rekomendasi penguatan sistem tenaga listrik berbasis keamanan adaptif dan berlapis.

Tabel 1. Perbandingan Metode Keamanan Jaringan pada Infrastruktur Energi

Metode Keamanan	Keunggulan Utama	Kelemahan / Tantangan	Efektivitas Deteksi
IDS/IPS Konvensional	Cepat mengenali pola serangan yang sudah dikenal	Kurang efektif terhadap serangan baru (*zero-day*)	Sedang
Deep Learning (CNN/LSTM)	Akurasi tinggi, mengenali pola kompleks dan non-linier	Membutuhkan data besar dan komputasi tinggi	Tinggi
Blockchain	Data tidak dapat dimanipulasi, sistem desentralisasi	Latensi tinggi, kurang optimal untuk aplikasi real-time	Tinggi (untuk integritas data)
Quantum Key Distribution	Keamanan absolut, anti-intersepsi	Biaya tinggi, sulit diimplementasikan secara luas	Sangat Tinggi (kriptografi)
MTD & Game Theory	Strategi adaptif, mampu mengantisipasi taktik penyerang	Kompleksitas dalam implementasi	Tinggi

Tabel ini menunjukkan bahwa tidak ada metode tunggal yang mampu mengatasi seluruh spektrum ancaman siber secara optimal. Oleh karena itu, pendekatan berlapis dan terintegrasi merupakan strategi yang paling efektif untuk melindungi sistem tenaga listrik modern. Integrasi teknologi AI, blockchain, dan sistem pertahanan prediktif perlu dibarengi dengan kebijakan operasional yang kuat, peningkatan kompetensi sumber daya manusia, serta pengembangan *testbed* realistis untuk pengujian sistem keamanan secara menyeluruh.

Pemahaman mendalam terhadap kelebihan dan keterbatasan setiap pendekatan memungkinkan perancang sistem dan pembuat kebijakan merumuskan solusi keamanan yang lebih tangguh, adaptif, dan berkelanjutan, selaras dengan dinamika sistem tenaga di masa depan.

Tabel 2. Ringkasan Hasil dan Pembahasan Penelitian dari Studi literatur

No.	Topik/Subtopik	Masalah Utama	Solusi / Pendekatan	Hasil / Temuan
1	SCADA & CPPS	Protokol usang dan rentan	IDS/IPS berlapis, autentikasi byte, enkripsi	Rentan terhadap serangan MiTM, DDoS, malware
2	Smart Meter	Ancaman privasi dan distribusi	Evaluasi protokol keamanan	Diperlukan pengamanan data sebagai prioritas
3	Serangan Hybrid dan Koordinasi	Sulit dideteksi, dampak sistemik	Deteksi berbasis Kalman, pendekatan AI	Efektif untuk mitigasi serangan terkoordinasi
4	Smart Grid	Konektivitas tinggi → risiko tinggi	Topology optimization, MTD, game theory	Perlunya taksonomi ancaman & sistem resiliensi

p-ISSN: 2775-4227
e-ISSN: 2775-4219

5	Energi Terbarukan & Power Electronics	Kompleksitas sistem meningkat	Penyimpanan energi, AI untuk stabilisasi	Simulasi tunjukkan peningkatan kestabilan
6	Deep Learning untuk Deteksi Ancaman	Kebutuhan deteksi real-time	CNN, LSTM (simulasi PSCAD)	Akurasi deteksi >98% untuk FDI, spoofing
7	Evaluasi Serangan (CIA)	Serangan pada integritas & ketersediaan	Analisis berdasarkan aspek CIA	Perlu standarisasi dan manajemen komunikasi
8	Teknologi Pendukung Keamanan	Ketergantungan IoT dan cloud	AI, Blockchain, SDN, IDS	Perkuat segmentasi & deteksi otomatis
9	Serangan DLAA–FDI	Serangan ringan tapi mematikan	Simulasi & bukti matematis	Gangguan pada sistem prosumer
10	IoT dalam Smart Grid	Keamanan rendah, interoperabilitas buruk	Kriptografi, protokol ringan, edge security	IoT jadi titik rawan yang butuh perhatian khusus
11	Mekanisme Terdesentralisasi	Sistem terlalu terpusat	Proteksi terdistribusi dan adaptif	Butuh pendekatan skala sistemik
12	Pengembangan Testbed	Kurangnya platform uji nyata	Testbed SCADA + HIL	Deteksi kerentanan, platform pelatihan
13	Quantum Key Distribution (QKD)	Kebutuhan enkripsi aman	Distribusi kunci berbasis kuantum	Cegah penyadapan, metrik dan use-case QKD
14	Interdependensi Siber-Fisik	Dampak serangan menyebar ke fisik	Co-simulation, digital twin	Visualisasi serangan & strategi pertahanan
15	Deteksi & Kontrol Pelacakan	Gangguan terhadap output pembangkit	PSO + Sliding Mode Observer (SMO)	Sistem tetap stabil meski ada gangguan
16	Load-Altering Attack (LAA)	Gangguan frekuensi sistemik	Simulasi transien berbasis arus injeksi	Deteksi efek LAA, risiko pemadaman total

Tabel 3. Perbedaan Teknologi, Pendekatan, dan Ancaman dalam Sistem Tenaga Modern

Aspek	SCADA Tradisional	Smart Grid Modern	CPPS (Cyber-Physical Power System)
Infrastruktur	Sistem tertutup, protokol lama (Modbus, DNP3)	Terbuka, berbasis IoT & komunikasi digital	Terintegrasi antara sistem fisik dan siber
Kontrol dan Monitoring	Lokal & manual, tidak real-time	Real-time dan otomatis berbasis sensor	Terdistribusi, adaptif dan berbasis AI
Keamanan Siber	Rentan, minim enkripsi dan autentikasi	Mulai menerapkan IDS/IPS, kriptografi	Kompleks, butuh pendekatan multi-layer
Jenis Ancaman Umum	Malware, serangan MiTM, akses ilegal	FDI, replay attack, spoofing GPS	Hybrid attacks (DLAA-FDI), serangan terkoordinasi
Kerentanan Utama	Protokol usang dan tidak terenkripsi	Perangkat IoT & komunikasi terbuka	Interdependensi antara dunia fisik & digital
Deteksi Ancaman	Manual dan reaktif	AI (CNN, LSTM), IDS berbasis rule & behavior	PSO, SMO, prediksi Kalman untuk deteksi dinamis
Respons Terhadap Serangan	Umumnya offline/manual	Semi-otomatis dengan peringatan dini	Real-time, adaptif, berbasis optimasi

p-ISSN: 2775-4227
e-ISSN: 2775-4219

Aspek	SCADA Tradisional	Smart Grid Modern	CPPS (Cyber-Physical Power System)
Sumber Energi	Umumnya terpusat (PLTA, PLTU)	Campuran, dominasi energi terbarukan	Sangat terdesentralisasi, banyak prosumer
Penggunaan IoT	Tidak digunakan	Digunakan luas pada smart meter, sensor	Kritis sebagai backbone komunikasi
Model Uji / Testbed	Terbatas, lebih pada analisis teoritis	Ada testbed digital untuk simulasi serangan	Kombinasi fisik-digital (HIL, co-simulation)
Keamanan Data	Bergantung pada isolasi fisik	Melibatkan enkripsi & autentikasi digital	Butuh solusi kuantum (QKD), blockchain
Pendekatan Inovatif	Jarang diperbarui	AI, SDN, edge computing mulai diterapkan	Deep Reinforcement Learning, digital twin
Ketergantungan Komunikasi	Rendah, jalur tertutup	Tinggi, menggunakan internet & cloud	Sangat tinggi dan kompleks
Tujuan Utama	Operasi stabil & terpusat	Efisiensi, fleksibilitas, kontrol desentralisasi	Ketahanan terhadap ancaman siber-fisik simultan

Tabel 4. Perbandingan Evolusi Sistem Tenaga Listrik

Aspek	SCADA Tradisional	Smart Grid	Cyber-Physical Power System (CPPS)
Arsitektur Sistem	Terpusat dan tertutup	Terdistribusi dan terbuka	Terintegrasi antara dunia fisik dan siber
Teknologi Komunikasi	Protokol lama (Modbus, DNP3), tidak terenkripsi	Komunikasi real-time via Internet dan sensor	IoT, edge/cloud computing, digital twin
Keamanan Siber	Minim, tidak mendukung enkripsi & autentikasi	IDS/IPS, kriptografi, standar keamanan mulai diterapkan	Sistem berlapis dengan AI, blockchain, QKD, dll
Jenis Ancaman Umum	Malware, akses tidak sah, MiTM	FDI, replay attack, spoofing GPS	Hybrid attacks, DLAA-FDI, coordinated cyber-physical attack
Respon terhadap Ancaman	Manual, setelah kejadian	Semi-otomatis dengan sistem peringatan	Deteksi dini dan respons adaptif real-time berbasis AI
Monitoring dan Kontrol	Terbatas, lokal	Monitoring real-time via smart meter	Otomatis, berbasis AI dan sistem prediktif
Sumber Energi	Pusat pembangkit besar (PLTU, PLTA)	Integrasi energi terbarukan (surya, angin)	Dikuasai prosumer & DER (Distributed Energy Resources)
Penggunaan IoT	Tidak ada	Digunakan pada smart meter, sensor	IoT sebagai tulang punggung komunikasi
Kebutuhan Infrastruktur Tambahan	Rendah	Menengah (komunikasi & komputasi)	Tinggi (storage, sensor, sistem AI, keamanan berlapis)

p-ISSN: 2775-4227
e-ISSN: 2775-4219

Aspek	SCADA Tradisional	Smart Grid	Cyber-Physical Power System (CPPS)
Contoh Teknologi Keamanan	Firewall dasar	IDS/IPS, kriptografi, SDN	QKD, blockchain, Deep RL, SMO, PSO
Platform Pengujian (Testbed)	Terbatas, lebih ke simulasi teoritis	Digital testbed, simulasi serangan	HIL, co-simulation, real-time emulation
Tujuan Utama Sistem	Operasi sistem yang stabil	Efisiensi, kontrol dinamis dan fleksibilitas	Ketahanan adaptif terhadap ancaman simultan

Penjelasan Tabel 2 : Ringkasan Hasil dan Pembahasan Penelitian dari Studi literatur

Tabel 1. menyajikan sintesis dari berbagai studi literatur mengenai keamanan sistem tenaga modern. Dapat disimpulkan bahwa berbagai komponen seperti SCADA, smart grid, hingga CPPS memiliki tantangan keamanan yang saling tumpang tindih, seperti kerentanan terhadap serangan berbasis komunikasi, ancaman pada data privasi, dan kesulitan dalam mendeteksi serangan secara real-time. Pola kesamaan ini menunjukkan bahwa pendekatan keamanan tidak dapat dilakukan secara parsial atau hanya pada satu komponen saja. Sebaliknya, dibutuhkan strategi sistemik yang menyatukan berbagai pendekatan keamanan siber seperti kriptografi, AI, IDS/IPS, serta mitigasi berbasis simulasi dan prediksi. Keterpaduan dan kolaborasi antar elemen dalam sistem tenaga menjadi faktor krusial dalam memperkuat ketahanan siber secara menyeluruh.

Penjelasan Tabel 3: Perbedaan Teknologi, Pendekatan, dan Ancaman dalam Sistem Tenaga Modern

Tabel 2. menguraikan perbedaan karakteristik antara sistem SCADA tradisional, smart grid modern, dan CPPS. Setiap sistem memiliki kompleksitas yang meningkat seiring transformasi digitalnya. SCADA tradisional, yang pada awalnya bersifat tertutup dan minim konektivitas digital, kini telah berevolusi menjadi sistem terbuka yang sangat terhubung dalam smart grid, hingga mencapai integrasi mendalam antara fisik dan siber dalam CPPS. Perbedaan tersebut tercermin dalam aspek kontrol, komunikasi, jenis serangan, dan pendekatan mitigasi. Secara khusus, CPPS menghadirkan tantangan keamanan paling signifikan karena melibatkan banyak entitas (prosumers, DER, perangkat IoT) dan bergantung pada infrastruktur komunikasi yang kompleks. Hal ini menegaskan pentingnya strategi keamanan yang bersifat adaptif, terdistribusi, dan didukung teknologi mutakhir seperti digital twin, AI, blockchain, serta enkripsi kuantum.

Penjelasan Tabel 4 : Perbandingan Evolusi Sistem Tenaga Listrik

Tabel 3. menggambarkan perjalanan evolusi sistem tenaga listrik dari SCADA ke Smart Grid hingga ke Cyber-Physical Power System (CPPS). Evolusi ini tidak hanya mencakup peningkatan teknologi komunikasi dan kontrol, tetapi juga berimplikasi langsung terhadap kerentanan siber. SCADA tradisional berfokus pada stabilitas dan pengendalian terpusat, sedangkan smart grid membawa fleksibilitas dan efisiensi melalui integrasi energi terbarukan dan IoT. CPPS, sebagai tahap paling lanjut, menghadirkan interkoneksi fisik-siber yang kompleks, menjadikannya sangat rentan terhadap serangan simultan dan terkoordinasi. Oleh karena itu, perancangan sistem keamanan siber harus berevolusi seiring transformasi arsitektur sistem tenaga, dengan mengedepankan pemantauan real-time, sistem prediktif, dan pendekatan holistik yang mampu menjawab tantangan operasional maupun keamanan yang semakin dinamis.

4. REKOMENDASI

Untuk memperkuat keamanan siber infrastruktur energi, khususnya pada sistem tenaga listrik dan smart grid, dibutuhkan pendekatan berlapis yang mencakup aspek teknologi, kebijakan, pelatihan, serta kolaborasi lintas sektor. Strategi utama meliputi:

a. Adopsi Teknologi Keamanan Canggih
   - Kecerdasan Buatan & Machine Learning: Digunakan untuk deteksi anomali, prediksi ancaman, serta pembelajaran adaptif berbasis data [35].
   - Blockchain: Menjamin integritas data dan transaksi yang tidak dapat dimanipulasi [44].
   - Software Defined Networking (SDN): Memungkinkan pengelolaan jaringan yang fleksibel dan responsif [47].
   - Quantum Cryptography & QKD: Memberikan jalur komunikasi yang sangat aman [21].
   - Digital Twins & Cloud SCADA: Digunakan untuk simulasi, pengujian sistem real-time, dan fleksibilitas operasional [40].

p-ISSN: 2775-4227
e-ISSN: 2775-4219

- Edge Computing & 5G: Mempercepat respons sistem namun perlu mitigasi terhadap kerentanan baru [50].
- Testbed Cyber-Physical (seperti HINT-Sec): Platform riset dan pelatihan yang realistis untuk menguji skenario serangan [30].

b. Peningkatan Standar, Kebijakan & Regulasi
- Penguatan Standar IoT: Meningkatkan enkripsi, autentikasi, dan kontrol akses pada perangkat pintar [42].
- Kerangka Regulasi Internasional untuk DER dan Smart Meters: Menjamin interoperabilitas, keamanan komunikasi, dan pemulihan pasca serangan [47][50].
- Audit dan Segmentasi Jaringan: Membatasi pergerakan lateral ancaman dan meningkatkan jejak digital untuk investigasi [43].

c. Ketahanan Sistem dan Pertahanan Adaptif
- Pertahanan Berlapis (Layered Security): Enkripsi, otentikasi multifaktor, IDS/IPS, firewall cerdas, dan deteksi intrusi berbasis AI [44].
- Moving Target Defense (MTD): Mengubah parameter sistem secara dinamis untuk menghindari deteksi oleh penyerang, termasuk DD-MTD untuk sistem AC [22].
- Penggunaan Energi Penyimpanan: Untuk stabilisasi sistem pasca serangan melalui algoritma penempatan optimal.
- Pemeliharaan Prediktif & Penilaian Kerentanan: Pencegahan dini melalui data historis dan analitik canggih.

d. Pendidikan, Pelatihan, dan Kesadaran Keamanan
- Pelatihan Intensif Operator: Terkait identifikasi dan penanganan insiden siber [36].
- Kurikulum Interdisipliner: Mencakup cybersecurity, kontrol sistem tenaga, dan komunikasi digital [35].
- Edukasi Pengguna Akhir: Meningkatkan kesadaran akan ancaman dan perlindungan perangkat pintar.

e. Kolaborasi dan Penelitian Lanjutan
- Kerjasama Akademisi-Industrialis-Pemerintah: Mendorong inovasi teknologi keamanan dan penyusunan kebijakan strategis [6].
- Simulasi dan Validasi Lapangan: Pengujian strategi dalam skala realistis untuk evaluasi efektivitas pertahanan [49].
- Model Serangan & Pertahanan Berbasis Game Theory: Simulasi interaksi antara penyerang dan pembela untuk meningkatkan strategi dinamis [35].
- Framework Keamanan Terintegrasi: Menggabungkan perlindungan IT dan OT dalam satu kerangka kerja.

f. Riset Strategis dan Fokus Masa Depan
- Keamanan DER & Microgrid: Pengembangan arsitektur komunikasi aman dan algoritma deteksi anomali [47].
- Ketahanan terhadap Serangan AI-enhanced dan Serangan Terkoordinasi: Melalui prediksi jalur serangan dan DSS berbasis data [49].
- Peningkatan Dataset & Validasi Eksperimen: Penyediaan data yang representatif serta pengujian laboratorium untuk generalisasi model deteksi [24][49].
- Keamanan Protokol Kritis (Modbus, Wi-Fi): Perbaikan otentikasi dan enkripsi untuk melindungi protokol lama [41].
- Standardisasi Global: Menyatukan pendekatan keamanan untuk smart meters dan sistem distribusi [50].

Keamanan siber infrastruktur tenaga listrik menuntut integrasi teknologi canggih, kebijakan yang proaktif, kolaborasi antar pemangku kepentingan, serta penguatan dari aspek manusia dan proses. Strategi adaptif dan berbasis data perlu dikembangkan untuk menghadapi ancaman siber yang semakin kompleks dan dinamis di era digital ini.

5. KESIMPULAN

Penelitian ini menunjukkan bahwa metode keamanan paling efektif dalam melindungi infrastruktur energi listrik adalah sistem deteksi intrusi (IDS), firewall cerdas, dan algoritma pembelajaran mesin. Pendekatan keamanan berlapis terbukti krusial dalam menghadapi beragam jenis serangan, terutama terhadap sistem seperti SCADA, smart grid, dan CPPS yang sangat rentan karena keterhubungan digitalnya.

Secara praktis, penerapan teknologi seperti AI, blockchain, dan enkripsi kuantum dapat meningkatkan ketahanan terhadap serangan siber kompleks dan terkoordinasi.

p-ISSN: 2775-4227
e-ISSN: 2775-4219

Untuk pengembangan ke depan, disarankan dilakukan penelitian lanjutan pada metode deteksi serangan berbasis AI yang lebih adaptif, termasuk pemanfaatan deep learning dan digital twin untuk simulasi dan respons real-time terhadap ancaman siber.

DAFTAR PUSTAKA

[1] S. Abdelkader *et al.*, "Securing modern power systems: Implementing comprehensive strategies to enhance resilience and reliability against cyber-attacks," Sep. 01, 2024, *Elsevier B.V.* doi: 10.1016/j.rineng.2024.102647.

[2] T. B. Prabowo and R. A. Sihaloho, "Analisis ketergantungan Indonesia pada teknologi asing dalam sektor energi dan dampaknya pada keamanan nasional," *Jurnal Lemhannas RI*, vol. 11, no. 1, pp. 72–82, May 2023, doi: 10.55960/jlri.v11i1.426.

[3] K. Tsantikidou and N. Sklavos, "Threats, Attacks, and Cryptography Frameworks of Cybersecurity in Critical Infrastructures," *Cryptography*, vol. 8, no. 1, Mar. 2024, doi: 10.3390/cryptography8010007.

[4] H. Satriyawan and S. Susanto, "Jurnal Restikom : Riset Teknik Informatika dan Komputer Optimasi Keamanan Smart Grid Melalui Autentikasi Dua Lapis: Meningkatkan Efisiensi dan Privasi dalam Era Digital," vol. 5, no. 3, pp. 319–333, 2023, [Online]. Available: https://restikom.nusaputra.ac.id

[5] Badan Siber dan Sandi Negara, *Peraturan Badan Siber dan Sandi Negara Nomor 5 Tahun 2020 tentang Rencana Strategis Badan Siber dan Sandi Negara Tahun 2020–2024*, 2020. [Online]. Available: https://bssn.go.id

[6] B. Achaal, M. Adda, M. Berger, H. Ibrahim, and A. Awde, "Study of smart grid cyber-security, examining architectures, communication networks, cyber-attacks, countermeasure techniques, and challenges," Dec. 01, 2024, *Springer Science and Business Media B.V.* doi: 10.1186/s42400-023-00200-w.

[7] B. Paul *et al.*, "Potential smart grid vulnerabilities to cyber attacks: Current threats and existing mitigation strategies," *Heliyon*, vol. 10, no. 19, p. e37980, Oct. 2024, doi: 10.1016/j.heliyon.2024.e37980.

[8] A. P. Yanuar, "Cyber war: Ancaman baru keamanan nasional dan internasional," *Jurnal Keamanan Nasional*, vol. 7, no. 1, pp. 23–35, Agustus 2021. [Online]. Tersedia: https://ejurnal.ubharajaya.ac.id/index.php/kamnas/article/view/1597

[9] T. V. Vimy *et al.*, "Ancaman serangan siber pada keamanan nasional Indonesia," *Jurnal Kewarganegaraan*, vol. 6, no. 1, Jun. 2022. doi: 10.31316/jk.v6i1.2989.

[10] A. A. R. Nasution and M. S. Hasibuan, "Analisis keamanan jaringan smart grid PLN menggunakan metode blockchain dalam konteks keamanan siber," *Journal of Computer Science and Informatics Engineering (CoSIE)*, vol. 3, no. 2, Apr. 2024, pp. 64–73. doi: 10.55537/cosie.v3i2.849.

[11] D. Aribowo, J. Damayanti, M. Sadewa, S. R. Nabila, dan Sarnata, "Risiko keamanan dan kerentanan jaringan transmisi listrik terhadap serangan siber pada infrastruktur energi terdistribusi," *Jurnal Surya Teknika*, vol. 11, no. 2, pp. 710–716, Des. 2024, doi: 10.37859/jst.v11i2.8311.

[12] S. Borenius, P. Gopalakrishnan, L. B. Tjernberg, and R. Kantola, "Expert-Guided Security Risk Assessment of Evolving Power Grids," *Energies (Basel)*, vol. 15, no. 9, May 2022, doi: 10.3390/en15093237.

[13] E. Soesanto *et al.*, "Analisis objek vital, keamanan file, dan keamanan cyber pada PT PLN," *IJM: Indonesian Journal of Multidisciplinary*, vol. 1, no. 1, 2023. [Online]. Available: https://journal.csspublishing.com/index.php/ijm/article/view/132

[14] A. Zibaeirad, F. Koleini, S. Bi, T. Hou, and T. Wang, "A comprehensive survey on the security of smart grid: Challenges, mitigations, and future research opportunities," *arXiv preprint*, arXiv:2407.07966, Jul. 2024, doi: 10.48550/arXiv.2407.07966.

[15] Z. A. Hussein dan M. N. Jassim, "Protecting renewable energy systems from cyber attacks and data breaches," *Int. J. Res. Publ. Rev.*, vol. 5, no. 8, pp. 3482–3487, Agustus 2024. [Online]. Available: https://ijrpr.com/uploads/V5ISSUE8/IJRPR32510.pdf

[16] R. Štefko, K. Eliáš, K. Glajc, A. Hyseni, F. Margita, and J. Šimčák, "Cybersecurity Challenges in the Power Sector: Analysing Attacks on Electrical Grids and Substations," in *2025 IEEE 23rd World Symposium on Applied Machine Intelligence and Informatics (SAMI)*, IEEE, Jan. 2025, pp. 000459–000464, doi: 10.1109/SAMI63904.2025.10883298.

[17] B. Pandey, N. Zhakiyev, M. S. Gaur, F. Tumenbayeva, S. Kumar, and P. Pandey, "Prediction of False Data Injection Attacks in Smart Grid using AdaBoost, Deep Learning, and KNN," in *2025 IEEE 4th*

p-ISSN: 2775-4227
e-ISSN: 2775-4219

International Conference on AI in Cybersecurity, ICAIC 2025, Institute of Electrical and Electronics Engineers Inc., 2025, doi: 10.1109/ICAIC63015.2025.10849233.

[18] P. Biswas *et al.*, "An Extensive and Methodical Review of Smart Grids for Sustainable Energy Management—Addressing Challenges with AI, Renewable Energy Integration and Leading-edge Technologies," *IEEE Access*, early access, 2025, doi: 10.1109/ACCESS.2025.3537651.

[19] P. Blazek, A. Bohacik, R. Fujdiak, V. Jurak, and M. Ptacek, "Smart Grids Transmission Network Testbed: Design, Deployment, and Beyond," *IEEE Open Journal of the Communications Society*, 2024, doi: 10.1109/OJCOMS.2024.3517340.

[20] V. Bobato, K. Thongmai, A. Goulart, and K. Butler-Purry, "Cyber security of a smart power distribution system – Cyber subsystem use case," in *2025 IEEE PES Grid Edge Technologies Conference & Exposition (Grid Edge)*, IEEE, 2025, doi: 10.1109/GRIDEDGE61154.2025.10887416.

[21] W. Grice, M. Olama, A. Lee, and P. Evans, "Quantum Key Distribution Applicability to Smart Grid Cybersecurity Systems," *IEEE Access*, 2025, doi: 10.1109/ACCESS.2025.3533942.

[22] M. Mohammadpourfard, A. Shefaei, and Y. Weng, "An Adaptive Moving-Target Defense Strategy for Dynamic Nonlinear Power Systems," *IEEE Trans Industr Inform*, 2025, doi: 10.1109/TII.2024.3522771.

[23] I. Zografopoulos *et al*., "Cyber-Physical Interdependence for Power System Operation and Control," *IEEE Trans. Smart Grid*, 2025, doi: 10.1109/TSG.2025.3538012.

[24] C. Sun, Q. Su, and J. Li, "Secure Tracking Control and Attack Detection for Power Cyber-Physical Systems based on Integrated Control Decision," *IEEE Transactions on Information Forensics and Security*, 2024, doi: 10.1109/TIFS.2024.3516557.

[25] G. Tian, Q. Z. Sun, and N. Song, "A Transient Simulation Framework for the Impact Analysis of Power System Load Altering Attacks," in *2025 IEEE PES Grid Edge Technologies Conference and Exposition, Grid Edge 2025*, Institute of Electrical and Electronics Engineers Inc., 2025. doi: 10.1109/GridEdge61154.2025.10887479.

[26] Z. Zhou and D. Duan, "Hybrid DLAA-FDI: A Practical New Cybersecurity Threat in the Era of High-power DERs," in *2025 IEEE PES Grid Edge Technologies Conference and Exposition, Grid Edge 2025*, Institute of Electrical and Electronics Engineers Inc., 2025. doi: 10.1109/GridEdge61154.2025.10887432.

[27] S. Amanlou *et al.*, "Cybersecurity Challenges in Smart Grid Systems: Current and Emerging Attacks, Opportunities, and Recommendations," *IEEE Open Journal of the Communications Society*, 2025, doi: 10.1109/OJCOMS.2025.3545153.

[28] M. A. S. P. Dayarathne *et al*., "Mitigating Cyber Risks in Smart Cyber-Physical Power Systems through Deep Learning and Hybrid Security Models," *IEEE Access*, 2025, doi: 10.1109/ACCESS.2025.3545637.

[29] A. Mughaid, S. Alzu'bi, A. A. A. Alkhatib, A. AlZioud, A. Al Ghazo, and I. AL-Aiash, "Simulation-based framework for authenticating SCADA systems and cyber threat security in edge-based autonomous environments," *Simul Model Pract Theory*, vol. 140, Apr. 2025, doi: 10.1016/j.simpat.2025.103078.

[30] K. Nam, K. Kwon, and A. Kim, "HINT-Sec: Hardware-in-the-loop nuclear power plant testbed for cyber security," *Progress in Nuclear Energy*, vol. 180, Feb. 2025, doi: 10.1016/j.pnucene.2024.105600.

[31] R. Kavikumar, O. M. Kwon, M. J. Park, and R. Sakthivel, "Dissipative constraint-based multi-area power system with time-varying delays and cyber-attacks," *ISA Trans*, 2025, doi: 10.1016/j.isatra.2025.01.018.

[32] D. Du *et al.*, "Distributed security state estimation-based carbon emissions and economic cost analysis for cyber–physical power systems under hybrid attacks," *Appl Energy*, vol. 353, Jan. 2024, doi: 10.1016/j.apenergy.2023.122001.

[33] S. Yang, K. W. Lao, H. Hui, J. Su, and S. Wang, "Secure frequency regulation in power system: A comprehensive defense strategy against FDI, DoS, and latency cyber-attacks," *Appl Energy*, vol. 379, Feb. 2025, doi: 10.1016/j.apenergy.2024.124772.

[34] M. Bakeer, A. Bakeer, G. Magdy, and M. M. Aly, "A new cyber-security approach for load frequency control of hybrid interconnected renewable power systems," *J Clean Prod*, vol. 425, Nov. 2023, doi: 10.1016/j.jclepro.2023.138866.

[35] Y. Feng, R. Huang, W. Zhao, P. Yin, and Y. Li, "A survey on coordinated attacks against cyber–physical power systems: Attack, detection, and defense methods," Apr. 01, 2025, *Elsevier Ltd*. doi: 10.1016/j.epsr.2024.111286.

[36] T. Zhao, H. Tu, R. Jin, Y. Xia, and F. Wang, "Improving resilience of cyber–physical power systems against cyber attacks through strategic energy storage deployment," *Reliab Eng Syst Saf*, vol. 252, Dec.

2024, doi: 10.1016/j.ress.2024.110438.

[37] O. O. Tooki and O. M. Popoola, "A critical review on intelligent-based techniques for detection and mitigation of cyberthreats and cascaded failures in cyber-physical power systems," Oct. 01, 2024, *Elsevier Ltd*, doi: 10.1016/j.ref.2024.100628.

[38] J. Marron, A. Gopstein, N. Bartol, and V. Feldman, "Cybersecurity framework smart grid profile," Gaithersburg, MD, Jul. 2019. doi: 10.6028/NIST.TN.2051.

[39] A. Plager, E. Olexa, D. Gardner, B. Torres, A. Hays, and A. Farraj, "A Study of SCADA System Vulnerabilities and Man-in-the-Middle Threats in Substation Operations," in *2025 IEEE Texas Power and Energy Conference, TPEC 2025*, Institute of Electrical and Electronics Engineers Inc., 2025, doi: 10.1109/TPEC63981.2025.10907190.

[40] S. M. Nahidul Islam *et al.*, "An Intelligent SCADA System for Power Distribution Network Cable Fault Detection with Real-Time Monitoring and Autonomous Maintenance," in *International Conference on Robotics, Electrical and Signal Processing Techniques*, Institute of Electrical and Electronics Engineers Inc., 2025, pp. 372–376, doi: 10.1109/ICREST63960.2025.10914481.

[41] M. Garcia and S. Kumar, "Experimentations for Enhancing Data Security Resilience of Energy Infrastructure," in *2025 IEEE 15th Annual Computing and Communication Workshop and Conference, CCWC 2025*, Institute of Electrical and Electronics Engineers Inc., 2025, pp. 257–261, doi: 10.1109/CCWC62904.2025.10903923.

[42] J. Mitchell, A. B. Mailewa, A. Akuthota, and T. Mohottalalage, "IoT-Driven Energy Management and Optimization: A Comprehensive Review and Case Study Analysis," in *2025 IEEE 15th Annual Computing and Communication Workshop and Conference, CCWC 2025*, Institute of Electrical and Electronics Engineers Inc., 2025, pp. 292–298, doi: 10.1109/CCWC62904.2025.10903553.

[43] A. Farraj, "On Using Zero Trust to Securing Industrial Control Systems in the Power Systems Industry," in *2025 IEEE Texas Power and Energy Conference, TPEC 2025*, Institute of Electrical and Electronics Engineers Inc., 2025, doi: 10.1109/TPEC63981.2025.10906998.

[44] S. Amanlou *et al.*, "Cybersecurity Challenges in Smart Grid Systems: Current and Emerging Attacks, Opportunities, and Recommendations," *IEEE Open Journal of the Communications Society*, 2025, doi: 10.1109/OJCOMS.2025.3545153.

[45] S. Tripathi, P. K. Verma, and G. Goswami, "A review on SMART GRID power system network," in *Proceedings of the 2020 9th International Conference on System Modeling and Advancement in Research Trends, SMART 2020*, Institute of Electrical and Electronics Engineers Inc., Dec. 2020, pp. 55–59. doi: 10.1109/SMART50582.2020.9337067.

[46] G. Chen, M. He, J. Gao, C. Liu, Y. Yin, and Q. Li, "Blockchain-Based Cyber Security and Advanced Distribution in Smart Grid," in *2021 IEEE 4th International Conference on Electronics Technology, ICET 2021*, Institute of Electrical and Electronics Engineers Inc., May 2021, pp. 1077–1080. doi: 10.1109/ICET51757.2021.9451130.

[47] J. Chen, J. Yan, A. Kemmeugne, M. Kassouf, and M. Debbabi, "Cybersecurity of distributed energy resource systems in the smart grid: A survey," *Appl Energy*, vol. 383, Apr. 2025, doi: 10.1016/j.apenergy.2025.125364.

[48] R. Marah, I. El Gabassi, S. Larioui, and H. Yatimi, "Security of Smart Grid Management of Smart Meter Protection," in *Proc. 1st Int. Conf. Innovative Res. Appl. Sci., Eng. Technol. (IRASET)*, Meknes, Morocco, 2020, pp. 1–5, doi: 10.1109/IRASET48871.2020.9092048.

[49] Ö. Sen *et al.*, "Simulation of multi-stage attack and defense mechanisms in smart grids," *International Journal of Critical Infrastructure Protection*, vol. 48, Mar. 2025, doi: 10.1016/j.ijcip.2024.100727.

[50] J. M. Nambundo, O. de Souza Martins Gomes, A. D. de Souza, and R. C. S. Machado, "Cybersecurity and Major Cyber Threats of Smart Meters: A Systematic Mapping Review," Mar. 01, 2025, *Multidisciplinary Digital Publishing Institute (MDPI)*, doi: 10.3390/en18061445.

[51] M. Amin, F. F. M. El-Sousy, G. A. A. Aziz, K. Gaber, and O. A. Mohammed, "CPS Attacks Mitigation Approaches on Power Electronic Systems with Security Challenges for Smart Grid Applications: A Review," *IEEE Access*, vol. 9, pp. 38571–38601, 2021, doi: 10.1109/ACCESS.2021.3063229.

[52] F. Alrefaei, "The Importance of Security in Cyber-Physical System," in Proc. 2020 IEEE 6th World Forum on Internet of Things (WF-IoT), New Orleans, LA, USA, Jun. 2–16, 2020. doi: 10.1109/WF-IoT48130.2020.9221155.