ISSN: 2354-6751

Risiko Keamanan dan Kerentanan Jaringan Transmisi Listrik Terhadap Serangan Siber pada Infrastruktur Energi Terdistribusi

Didik Aribowo, Jahra Damayanti, Muhamad Sadewa*, Syafa Raihanun Nabila, Sarnata
Universitas Sultan Ageng Tirtayasa
Jl. Ciwaru Raya, Cipare, Kec. Serang, Kota Serang, Banten 42117
E-mail: *2283220048@untirta.ac.id**

Abstract

Cybersecurity is a major challenge for energy infrastructure in remote areas that rely on distributed power grids. Limited resources and lower levels of monitoring compared to urban areas increase vulnerability to cyberattacks. This study analyzes the key risks faced by power transmission networks in remote areas, including restricted physical access, the use of outdated and vulnerable protocols, and insufficient network segmentation. To address these challenges, this research recommends a layered mitigation strategy, including data encryption, multi-factor authentication, network segmentation, and the adoption of blockchain technology. Additionally, training local staff and regularly updating software are crucial steps in enhancing network security. This study employs a literature review method, gathering and analyzing information from various sources such as books, journals, articles, and previous research findings. Data processing is conducted systematically to identify challenges and applicable solutions to improve the reliability of energy infrastructure in remote areas. The implementation of these recommended strategies is expected to reduce cybersecurity risks and enhance the security of power grids in such regions.

Keywords: *Cybersecurity, Distributed Networks, Remote Areas, blockchain, Energy Infrastructure.*

Abstrak

Keamanan siber merupakan tantangan besar bagi infrastruktur energi di daerah terpencil yang menggunakan jaringan listrik terdistribusi. Keterbatasan sumber daya dan pengawasan yang lebih rendah dibandingkan wilayah perkotaan meningkatkan kerentanan terhadap serangan siber. Penelitian ini menganalisis risiko utama yang dihadapi jaringan transmisi listrik di daerah terpencil, termasuk akses fisik yang terbatas, penggunaan protokol lama yang rentan, serta kurangnya segmentasi jaringan. Untuk mengatasi tantangan ini, penelitian ini merekomendasikan strategi mitigasi berlapis, seperti enkripsi data, autentikasi multifaktor, segmentasi jaringan, serta pemanfaatan teknologi blockchain. Selain itu, pelatihan staf lokal dan pembaruan perangkat lunak secara berkala menjadi langkah penting dalam meningkatkan keamanan jaringan. Penelitian ini dilakukan dengan metode studi literatur, yaitu mengumpulkan dan menganalisis informasi dari berbagai sumber pustaka, seperti buku, jurnal, artikel, dan hasil penelitian sebelumnya. Pengolahan data dilakukan secara sistematis untuk mengidentifikasi tantangan serta solusi yang dapat diterapkan guna meningkatkan keandalan infrastruktur energi di daerah terpencil. Implementasi strategi yang direkomendasikan diharapkan dapat mengurangi risiko serangan siber dan meningkatkan keamanan jaringan listrik di wilayah tersebut.

Kata kunci: *Keamanan Siber, Jaringan Terdistribusi, Daerah Terpencil, Blockchain, Infrastruktur Energi.*

1. Pendahuluan

Listrik merupakan elemen penting dalam kehidupan modern, di mana hampir semua aktivitas manusia melibatkan penggunaan perangkat elektronik yang bergantung pada energi listrik. Seiring meningkatnya ketergantungan pada sistem tenaga listrik, infrastruktur energi, terutama di daerah terpencil dengan jaringan listrik terdistribusi (decentralized), menghadapi tantangan besar dalam aspek keamanan siber.

Jaringan listrik di daerah terpencil cenderung memiliki sistem keamanan yang lebih lemah dibandingkan dengan jaringan di perkotaan, karena keterbatasan sumber daya dan pengawasan yang lebih rendah. Hal ini meningkatkan risiko serangan siber terhadap sistem transmisi listrik,

yang dapat mengganggu pasokan energi dan mengancam keandalan infrastruktur energi. Oleh karena itu, upaya peningkatan keamanan siber dalam sistem transmisi listrik menjadi krusial untuk memastikan kontinuitas layanan energi yang stabil dan aman.

Salah satu teknologi yang dapat berkontribusi dalam meningkatkan keamanan siber adalah blockchain. Blockchain menawarkan sistem yang terdesentralisasi, transparan, dan sulit ditembus, yang dapat digunakan untuk meningkatkan keamanan data dalam jaringan listrik. Dengan penerapan yang tepat, blockchain dapat membantu mengamankan transaksi data dalam sistem tenaga listrik serta mencegah manipulasi atau akses tidak sah terhadap jaringan.

Transmisi tenaga listrik diklasifikasikan ke dalam beberapa kategori. Kategori pertama adalah transmisi dengan tegangan 500 kV, yang dianggap sangat tinggi. Di Indonesia, sistem 500 kV masih digunakan. Kategori kedua adalah transmisi dengan tegangan 150 kV, dan kategori ketiga adalah transmisi 75 kV. Tegangan di bawah 75 kV kemudian disebut sebagai distribusi tenaga listrik.

Teknologi masa depan seperti blockchain memiliki potensi besar untuk mengubah secara signifikan cara pemasaran listrik dan bagaimana konsumen beroperasi. Ketika digabungkan dengan kontrak pintar, teknologi blockchain dapat menyediakan sistem yang transparan, aman, dan sulit ditembus, sehingga mampu menciptakan peluang bisnis baru. Fitur ini membuat blockchain berpotensi menjadi alat yang berguna untuk mengatur dan mengontrol jaringan serta pasar listrik yang semakin kompleks dan terdesentralisasi di masa depan. Ini akan memungkinkan integrasi Sumber Energi Terbarukan (RES) dalam skala besar dengan biaya rendah secara lebih menguntungkan, efisien, dan efektif bagi semua pihak di pasar.

Penelitian ini berfokus pada analisis risiko keamanan dan kerentanan jaringan transmisi listrik terhadap serangan siber serta strategi mitigasi yang dapat diterapkan untuk meningkatkan keamanan sistem tenaga listrik di daerah terpencil.

2. Metodologi

Penelitian ini menggunakan metode **studi literatur**, yaitu pendekatan yang dilakukan dengan mengumpulkan dan menganalisis berbagai sumber pustaka yang relevan untuk mengidentifikasi risiko keamanan siber pada jaringan transmisi listrik di daerah terpencil serta strategi mitigasi yang dapat diterapkan.

Pengumpulan Data

Data dalam penelitian ini dikumpulkan dari berbagai sumber yang memiliki kredibilitas tinggi, termasuk jurnal ilmiah, buku referensi, laporan penelitian, serta artikel akademik yang dipublikasikan dalam konferensi atau jurnal bereputasi. Untuk memastikan validitas sumber, literatur yang digunakan dalam penelitian ini dipilih berdasarkan kriteria berikut:

- Diterbitkan dalam jurnal terindeks dan bereputasi (misalnya, IEEE, Elsevier, Springer, atau jurnal nasional yang telah terakreditasi).
- Memiliki relevansi langsung dengan tema keamanan siber, infrastruktur energi, dan teknologi blockchain dalam sistem transmisi listrik.
- Menggunakan data empiris atau kajian akademik yang dapat dipertanggungjawabkan.

Selain itu, referensi yang lebih baru (dalam kurun waktu 5–10 tahun terakhir) lebih diutamakan untuk memastikan bahwa penelitian ini menggunakan informasi terkini tentang tantangan dan solusi keamanan siber dalam infrastruktur listrik.

Analisis Data dan Relevansi Literatur

Literatur yang telah dikumpulkan dievaluasi berdasarkan relevansi dengan topik penelitian. Analisis dilakukan dengan pendekatan **komparatif dan sintesis tematik**, yang mencakup:

Identifikasi Risiko Keamanan Siber

- Meninjau berbagai studi kasus tentang serangan siber terhadap infrastruktur energi.
- Mengidentifikasi pola dan faktor utama yang menyebabkan kerentanan jaringan transmisi listrik.

Evaluasi Teknologi Mitigasi

- Membandingkan berbagai strategi mitigasi keamanan siber, seperti enkripsi data, autentikasi multifaktor, segmentasi jaringan, dan penerapan blockchain.
- Menganalisis efektivitas teknologi yang telah diterapkan dalam sistem transmisi listrik berdasarkan literatur yang ada.

Integrasi Blockchain dalam Keamanan Siber

- Mengkaji bagaimana teknologi blockchain dapat meningkatkan keamanan siber dalam jaringan transmisi listrik.
- Meninjau kelebihan dan keterbatasan implementasi blockchain dalam sistem tenaga listrik yang terdistribusi.

3. Hasil dan Pembahasan

Hasil Penelitian

Tingkat Kerentanan Serangan Siber

Adapun beberapa tingkatan dalam kerentanan serangan siber yang ada pada daerah terpencil:

1. Akses Fisik Terbatas (Physical Access)
   Infrastruktur listrik di wilayah terpencil seringkali tidak memiliki pengawasan fisik yang kuat, seperti pagar pengaman atau sistem pengawasan video. Penyerang yang dapat mengakses lokasi fisik ini bisa menyusup ke jaringan dengan mudah dan mengakses perangkat kritikal seperti PLC atau sensor. Hal ini meningkatkan kerentanan terhadap manipulasi fisik dan serangan siber.
2. Pemeliharaan Jarak Jauh (Remote Maintenance Access)
   Di banyak wilayah terpencil, akses pemeliharaan dilakukan secara jarak jauh melalui jaringan internet atau VPN. Jika akses ini tidak dilindungi dengan baik, seperti melalui enkripsi atau otentikasi yang kuat, jaringan bisa rentan terhadap serangan peretas yang mengeksploitasi akses jarak jauh ini.
3. Interkoneksi Jaringan Terbatas (Limited Network Separation)
   Wilayah terpencil biasanya memiliki infrastruktur komunikasi yang lebih terbatas dibandingkan dengan wilayah perkotaan. Jaringan antara sistem operasi dan jaringan kantor mungkin tidak memiliki pemisahan yang memadai, memungkinkan pergerakan lateral (lateral movement) bagi penyerang dari satu bagian jaringan ke bagian lain.
4. Keterbatasan Sumber Daya untuk Keamanan (Limited Security Resources)
   Operator di daerah terpencil seringkali memiliki keterbatasan dalam hal sumber daya keamanan siber. Ini bisa mencakup keterbatasan dalam perangkat keras modern yang mendukung protokol keamanan terbaru, serta kurangnya personel keamanan siber yang berpengalaman.
5. Kegagalan atau Manipulasi Protokol Lama (Legacy Protocols Vulnerability)
   Infrastruktur di daerah terpencil mungkin masih menggunakan protokol lama yang tidak dirancang dengan keamanan siber yang memadai, seperti DNP3 atau IEC 60870-5-104, yang rentan terhadap serangan seperti man-in-the-middle, spoofing, dan replay attacks.

Masing-masing dari poin di atas mengindikasikan bahwa infrastruktur di wilayah terpencil sangat rentan terhadap berbagai jenis serangan siber, baik yang bersifat fisik maupun melalui akses jaringan.

Analisis Ancaman Siber

Keamanan siber adalah upaya penerapan teknologi, proses, dan kontrol untuk melindungi sistem, jaringan, program, perangkat, dan data dari ancaman serangan siber. Tujuan dari

keamanan siber adalah untuk mengurangi risiko serangan dunia maya dan melindungi infrastruktur penting dari eksploitasi yang dilakukan terhadap sistem, jaringan, dan teknologi oleh virus atau aplikasi dari peretas yang tidak berwenang (Yulianto *et al.*, 2022). Terdapat lima jenis utama dari keamanan siber, yang dijelaskan sebagai berikut:

1. Keamanan Siber untuk Infrastruktur kritis sangat penting pada daerah terpencil karena infrastruktur ini cenderung lebih rentan terhadap serangan, terutama karena sistem SCADA (Supervisory Control and Data Acquisition atau sistem pengawasan dan pengumpulan data) sering bergantung pada perangkat lunak yang lebih usang. Penyedia layanan penting di sektor-sektor seperti energi, transportasi, kesehatan, air, dan infrastruktur digital di Inggris, serta penyedia layanan digital, harus mematuhi Peraturan NIS (Network and Information Systems Regulations 2018). Di antara aturan yang ada, kebijakan nasional mengharuskan penerapan langkah-langkah keamanan teknis untuk melindungi objek vital nasional, instansi, kementerian, dan lembaga agar dapat menjaga keamanan data mereka.
2. Keamanan Jaringan. Keamanan jaringan mencakup penanganan kerentanan yang dapat memengaruhi sistem operasi dan arsitektur jaringan, termasuk server dan host, firewall, titik akses nirkabel, serta protokol jaringan.
3. Keamanan Cloud. Keamanan cloud berfokus pada perlindungan data, aplikasi, dan infrastruktur yang berada di lingkungan cloud.
4. Keamanan IoT (Internet of Things). Keamanan IoT berkaitan dengan melindungi perangkat pintar dan jaringan yang terhubung ke ekosistem IoT. Perangkat IoT mencakup berbagai hal yang dapat terhubung ke Internet tanpa interaksi manusia, seperti alarm kebakaran pintar, lampu, termostat, dan perangkat lainnya.
5. Keamanan Aplikasi. Keamanan aplikasi berkaitan dengan penanganan kerentanan yang timbul akibat proses pengembangan yang tidak aman dalam desain, pengkodean, dan peluncuran perangkat lunak atau situs web.

Pada 23 Desember 2015, terjadi pemadaman listrik yang tidak terencana di Ukraina, yang berdampak pada banyak pelanggan di wilayah tersebut. Selain insiden tersebut, dilaporkan juga adanya malware yang ditemukan di beberapa perusahaan Ukraina yang bergerak di berbagai sektor infrastruktur kritis. Berdasarkan laporan publik, malware yang dikenal sebagai BlackEnergy (BE) ditemukan di jaringan komputer perusahaan-perusahaan ini. Namun, peran BE dalam insiden ini belum dapat dipastikan dan masih membutuhkan analisis teknis yang lebih mendalam ada **23 Desember 2015**, Ukraina mengalami serangan siber yang menyebabkan pemadaman listrik di beberapa wilayah. Investigasi menemukan bahwa peretas menggunakan malware **BlackEnergy** untuk menginfeksi jaringan kontrol industri. Serangan ini menargetkan **sistem Supervisory Control and Data Acquisition (SCADA)**, yang mengontrol distribusi listrik, sehingga memungkinkan peretas untuk mematikan pasokan listrik secara jarak jauh.

Konteks penelitian ini menunjukkan bahwa serangan serupa berpotensi terjadi di daerah terpencil dengan keamanan jaringan yang lebih lemah. **Kelemahan** dalam pemeliharaan jarak jauh, kurangnya segmentasi jaringan, serta penggunaan perangkat lunak lama seperti yang terjadi di Ukraina juga ditemukan dalam jaringan transmisi listrik di daerah terpencil. Oleh karena itu, strategi mitigasi yang lebih kuat harus diterapkan untuk mencegah kejadian serupa. Berikut adalah beberapa kerentanan teknologi energi terbarukan terhadap ancaman siber:

1. Keamanan siber sering kali tidak menjadi prioritas pada fase perancangan di banyak industri energi terbarukan yang saat ini beroperasi.
2. Industri energi terbarukan cenderung menggunakan Sistem SCADA dan CCTV dengan kualitas rendah atau murah yang tersedia di pasaran.

3. Pemilihan komponen utama sering dilakukan tanpa mempertimbangkan aspek keamanan siber.
4. Belum ada kebijakan atau regulasi khusus terkait keamanan siber yang harus dipatuhi dalam sektor energi terbarukan.
5. Pembeli dan konsultan teknis di industri energi terbarukan umumnya tidak mengevaluasi keamanan siber dari tahap transaksi, instalasi, penyelesaian, hingga penerimaan.
6. Salah satu kekhawatiran terbesar di sektor energi terbarukan adalah risiko keamanan siber yang mengancam rantai pasokannya.

Penyedia energi terbarukan perlu menerapkan pendekatan yang lebih hati-hati terhadap rantai pasokan mereka. Pengoperasi energi terbarukan harus banyak berdiskusi dengan pemasok dan industri energi terbarukan, serta memastikan peningkatan pemeliharaan dilakukan secara rutin jika diperlukan. Saat ini, banyak perusahaan energi di seluruh dunia semakin mendorong pelanggan untuk memasang pengukur pintar (smart meter) dan sensor lainnya. Namun, perangkat seperti pengukur pintar dan IoT rentan terhadap serangan siber karena dapat menjadi pintu masuk ke jaringan dan digunakan oleh penjahat siber untuk membangun botnet. Para eksekutif perusahaan energi perlu mengambil langkah taktis terkait keamanan IoT, karena sulit bagi pengguna untuk memperbaiki celah keamanan perangkat ini. Oleh karena itu, diperlukan regulasi dan kebijakan, seperti undang-undang yang mendukung keamanan desain, untuk meningkatkan keamanan siber. Penelitian lebih lanjut tentang strategi mitigasi risiko dan rekomendasi kebijakan juga sangat diperlukan.

Strategi Efektif Memperkuat Keamanan Siber

Strategi mitigasi yang efektif untuk memperkuat keamanan siber pada jaringan transmisi listrik di daerah terpencil melibatkan pendekatan berlapis yang mencakup teknologi, kebijakan, dan pelatihan. Pertama, penerapan enkripsi data dan autentikasi multifaktor sangat penting untuk melindungi akses ke sistem kontrol jaringan. Sistem deteksi intrusi (IDS) dan firewall juga harus dipasang untuk memantau dan mencegah serangan siber. Mengingat keterbatasan infrastruktur di daerah terpencil, penggunaan teknologi komunikasi berbasis satelit atau mesh network yang aman dapat meningkatkan redundansi dan memastikan kestabilan jaringan. Selain itu, penting untuk menerapkan pembaruan perangkat lunak secara berkala guna menambal kerentanan. Di sisi kebijakan, diperlukan standar keamanan yang ketat, serta prosedur respons cepat terhadap insiden yang telah disusun dan diuji secara rutin. Pelatihan berkelanjutan bagi staf operasional di daerah terpencil juga krusial untuk memastikan mereka siap menghadapi ancaman siber dan mematuhi protokol keamanan.

Pembahasan

Konsep Keamanan Siber

Keamanan siber pada infrastruktur listrik di daerah terpencil merupakan elemen penting dalam menjaga kestabilan jaringan energi dan melindungi dari serangan siber. Di daerah-daerah ini, langkah pertama adalah memperkuat **pengamanan fisik**, karena infrastruktur seperti gardu listrik seringkali tidak diawasi secara langsung. Penggunaan sensor gerak dan kamera pengawas bisa membantu mencegah akses fisik yang tidak sah (Nasution & Hasiuan, 2024). elain itu, **segmentasi jaringan** harus diterapkan untuk memisahkan jaringan kontrol operasional (OT) dari jaringan informasi (IT). Hal ini memastikan bahwa meskipun terjadi pelanggaran keamanan pada satu bagian jaringan, serangan tidak dapat dengan mudah menyebar ke seluruh sistem (Ernst *et al.*, 2021). **Manajemen akses jarak jauh** sangat penting dalam konteks daerah terpencil, di mana akses fisik ke infrastruktur sering dilakukan melalui jaringan. Penggunaan otentikasi multifaktor (MFA) dan jaringan pribadi virtual (VPN) yang aman bisa membantu mengamankan akses tersebut.

Penerapan Blockchain dan Teknologi Modern untuk Keamanan Siber di Daerah Terpencil

Untuk mengatasi tantangan keamanan siber dalam jaringan transmisi listrik di daerah terpencil, beberapa teknologi modern dapat diterapkan:

1. **Blockchain untuk Keamanan Data dan Kontrol Jaringan**

- Menggunakan **blockchain** untuk mencatat transaksi data dan operasi jaringan secara terdesentralisasi, sehingga sulit dimanipulasi oleh peretas.
- Mengintegrasikan blockchain dengan **kontrak pintar (smart contracts)** untuk mengotomatiskan proses validasi keamanan dalam sistem listrik.
- Memanfaatkan **teknologi blockchain dalam pemantauan akses jarak jauh**, sehingga setiap perubahan dalam jaringan tercatat secara transparan dan tidak dapat diubah.

2. **Segmentasi Jaringan dengan Sistem Zero Trust**
   - Menerapkan **Zero Trust Architecture (ZTA)** yang mengharuskan verifikasi akses setiap kali pengguna atau sistem mencoba mengakses jaringan.
   - Memisahkan jaringan operasional dan administrasi untuk mencegah peretas berpindah dari satu sistem ke sistem lainnya.
3. **Deteksi Ancaman dengan Kecerdasan Buatan (AI) dan Machine Learning**
   - Menggunakan AI untuk **mendeteksi anomali dalam lalu lintas jaringan**, yang dapat menunjukkan adanya upaya peretasan.
   - Menerapkan sistem Intrusion Detection System (IDS) berbasis machine **learning** untuk mengidentifikasi pola serangan baru.
4. **Peningkatan Enkripsi dan Autentikasi**
   - Menggunakan **enkripsi end-to-end** dalam komunikasi data antar perangkat transmisi listrik.
   - Menerapkan autentikasi multifaktor (MFA) untuk membatasi akses hanya kepada pengguna yang sah.

4. Simpulan

Penelitian ini menunjukkan bahwa jaringan transmisi listrik di daerah terpencil memiliki kerentanan tinggi terhadap serangan siber akibat keterbatasan sumber daya, kurangnya pengawasan, serta penggunaan teknologi lama yang rentan. Untuk mengurangi risiko tersebut, diperlukan penerapan strategi mitigasi seperti segmentasi jaringan, autentikasi multifaktor, enkripsi data, serta integrasi teknologi blockchain untuk meningkatkan transparansi dan keamanan sistem.

Hasil penelitian ini memiliki implikasi praktis bagi berbagai pihak. Bagi operator jaringan listrik, penting untuk mengadopsi sistem keamanan berlapis dengan menerapkan teknologi deteksi ancaman berbasis kecerdasan buatan serta meningkatkan pelatihan bagi tenaga teknis di daerah terpencil agar lebih siap menghadapi ancaman siber. Sementara itu, bagi pembuat kebijakan, diperlukan regulasi yang lebih ketat terkait standar keamanan siber dalam infrastruktur energi, khususnya bagi sistem yang beroperasi di wilayah dengan pengawasan terbatas. Insentif juga dapat diberikan untuk mendorong modernisasi teknologi transmisi listrik agar lebih aman dan andal. Selain itu, penelitian lanjutan masih diperlukan untuk mengevaluasi efektivitas blockchain dan teknologi lainnya dalam konteks infrastruktur listrik yang memiliki keterbatasan sumber daya. Dengan menerapkan rekomendasi ini, keamanan dan keandalan jaringan transmisi listrik di daerah terpencil dapat ditingkatkan, mengurangi risiko serangan siber, serta memastikan pasokan listrik yang lebih stabil bagi masyarakat.

Daftar Pustaka

[1] Z. P. S. L. P. Syiska Yana, "Pengaruh Pemasangan Static Var Compensator Pada," *Jurnal Nasional Teknik Elektro*, Vol. 5, No. 1, P. 2016, 2016.

[2] P. S. S. A. Yogi Syahputra Aritonang, "Inovasi Dan Tantangan Dalam Pengembangan Sistem Transmisi Tenaga Listrik Berbasis Teknologi Tinggi Ultra High Voltage Untuk Teknologi Tinggi Ultra High Voltage Untuk Teknologi Tinggi Ultra High Voltage Untuk Meningkatkan Keandalan Dan Efisiensi," *JITET (Jurnal Informatika Dan Teknik Elektro Terapan)*, 2024.

[3] L. N. Widyastuti, "Analisis Gangguan Sistem Transmisi Listrik Menggunakan Metode Root Cause Analysis (Rca)," Industrial Engineering Online Journal, 2014.

[4] P. Doloksaribu, "Analisa Keandalan Sistem Distribusi Tenaga Listrik," Jurnal Teknik Elektro Univ. Cendrawasih, Vol. 1, Pp. 20-25, 2010.

[5] E. K. B. H. I. &. H. Raphael, "Cybersecurity In Power Grids: Challenges And Opportunities," Sensors, Pp. 1-19, 2021.

[6] A. A. N. H. S. M. S. A. M. &. M. M. Sari, "Tantangan Dan Peluang Implementasi Teknologi Dalam," Jurnal Pendidikan Dan Pengajaran, Pp. 196-204, 2024.

[7] A. F. D. N. S. R. N. Y. &. D. M. Awaludin, "Peluang Dan Ancaman Kerja Sama Di Sektor Energi Dan Kebijakan," Jurnal Ekonomi Dan Bisnis Digital, Pp. 138-146, 2024.

[8] I. M. M. K. Astawa, "Metodologi Penilaian Kerentanan Pada Infrasruktur Kritikal Nasional," Seminar Nasional Aplikasi Teknologi Informasi, Pp. 67-73, 2019.

[9] M. F. R. B. &. I. A. I. Fadhlulloh, "Analisis Keamanan Jaringan Pada Smart Kwh Meter Berbasis Internet Of Things (IOT)," E-Proceeding Of Engineering, P. 3183, Agustus 2020.

[10] A. A. R. &. H. M. S. Nasution, "Analisis Keamanan Jaringan Smart Grid PLN Menggunakan Metode Blockchain Dalam Konteks Kemananan Cyber," Journal Of Computer Science And Informatics Engineering (Cosie), Pp. 64-73, April 2024.

[11] J. T. S. A. Y. &. I. A. M. Yulianto, "Analisis Potensi Ancaman Asimetris Berdasarkan Kerentanan Keamanan Siber Sektor Industri Energi Baru Terbarukan (EBT)," Jurnal Kewarganegaraan, September 2022.

[12] A. Subagyo, "Sinergi Dalam Menghadapi Ancaman Cyber Warfare Synergy In Facing Of Cyber Warfare Threat," Jurnal Pertahanan, Pp. 89-108, April 2015.

[13] F. J. Haluana'a, " Optimisasi Jaringan Energi Listrik Untuk Meningkatkan Efisiensi Dan Keberlanjutan," Writebox, Pp. 1-7, 2023.

[14] Y. W. &. K. D. Pratama, "Implementasi Blockchain Dalam Aplikasi Pemilu," International Journal Of Educational Resources, Pp. 242-254, 2021.

[15] G. J. R. E. Dileep, "A Survey On Smart Grid Technologies And Applications," Renewable Energy, Pp. 2589-2625, 2020.

[16] T. T. M. C. S. D. &. A. K. Plėta, "Cyber-Attacks To Critical Energy," Infrastructure And Management Issues: Overview Of Selected Cases, 2020.

[17] P. D. V. S. D. C. M. S. &. B. I. Samarati, "Cloud Security: Issues," And Concerns , Pp. 1-14, 2016.

[18] M. &. V. K. Chichester: Wiley.Tahaei, "A Survey On Developer-Centred Security," European Symposium On Security And Privacy Workshops (Euros&PW), Pp. 129-138, Juni 2019.