Teknik: Jurnal Ilmu Teknik dan Informatika
Volume 4 Nomor 2 Oktober 2024
e-ISSN: 2798-2513; p-ISSN: 2808-8751, Hal 09-16
DOI: https://doi.org/10.51903/teknik
Available online at: https://journal.stiestekom.ac.id/index.php/TEKNIK

Perancangan Sistem Keamanan Jaringan Berbasis Cybersecurity untuk Mitigasi Ancaman Siber pada Infrastruktur TI: Studi Kasus di Indonesia

Puteri Ananda Khairunnisa[1], Norul Annisa[2], Yukandri[3] Jadiaman Parhusip[4]
[1234]Universitas Palangka Raya, Palangka Raya, Indonesia

Email: [1]puterianandа11@gmail.com, [2]norulannisa107@gmail.com,[3]yukandri01@gmail.com, [4] parhusip.jadiaman@it.upr.ac.id

Alamat Kampus : Jl. Yos Sudarso, Palangka, Kec. Jekan Raya, Kota Palangka Raya, Kalimantan Tengah 74874

Korespondensi Penulis: puterianandа11@gmail.com

Abstract. *This study aims to design a cybersecurity-based network security system that is effective in reducing cyber threats to Information Technology (IT) infrastructure in Indonesia. Along with the increasing number of cyber attacks that attack various sectors, including government, banking, and health, this country faces a major challenge in maintaining data integrity and security. Based on data from the National Cyber and Crypto Agency (BSSN) and the AwanPintar.id report, cyber threats such as malware, ransomware, and DDoS are increasingly rampant, causing significant losses to the IT sector. Therefore, designing a robust security system that complies with national security regulations is important. This study uses a combination of approaches between existing network security technologies, such as the Intrusion Detection System (IDS) SNORT, Port Knocking, and the application of Artificial Intelligence (AI) in detecting behavioral-based threats. The results of the study show that this approach can not only improve detection and response to cyber threats, but also comply with the regulations set by BSSN. The proposed system is expected to reduce losses caused by cyber attacks and improve the security of IT infrastructure in Indonesia.*
Keywords: *Cybersecurity, Network Security, IT Infrastructure, Snort*
Abstrak. Penelitian ini dimaksudkan untuk merancang sistem keamanan jaringan berbasis keamanan Siber yang efektif dalam mengurangi ancaman siber pada infrastruktur Teknologi Informasi (TI) di Indonesia. Seiring dengan meningkatnya serangan siber yang menyerang sektor-sektor beragam, termasuk pemerintahan, perbankan, dan kesehatan, negara ini menghadapi tantangan besar dalam menjaga integritas dan keamanan data. Berdasarkan data dari Badan Siber dan Sandi Negara (BSSN) dan laporan AwanPintar.id, ancaman siber seperti malware, ransomware, dan DDoS semakin meningkat, yang menyebabkan kerugian signifikan pada sektor TI. Oleh karena itu, perancangan sistem keamanan yang kuat dan sesuai dengan regulasi keamanan nasional sangat diperlukan. Penelitian ini menggunakan kombinasi pendekatan antara teknologi keamanan jaringan yang telah ada, seperti Intrusion Detection Systems (IDS) SNORT, Port Knocking, dan penerapan Artificial Intelligence (AI) dalam mendeteksi ancaman berbasis perilaku. Hasil penelitian menunjukkan bahwa pendekatan ini tidak hanya dapat meningkatkan deteksi dan respons terhadap ancaman siber, tetapi juga mematuhi regulasi yang ditetapkan oleh BSSN. Sistem yang diusulkan diharapkan dapat mengurangi kerugian yang ditimbulkan oleh serangan siber dan meningkatkan keamanan infrastruktur TI di Indonesia.
Kata kunci: Cybersecurity, Keamanan jaringan, Infrastruktur TI, Snort

Received: September 11, 2024; Revised: September 18, 2024; Accepted: Oktober 12, 2024; Published: November 24, 2024;
*puterianandа11@gmail.com

1. LATAR BELAKANG

Keamanan siber merupakan tantangan besar di Indonesia karena ancaman terhadap infrastruktur Teknologi Informasi (TI) semakin meningkat di sektor-sektor seperti pemerintahan, perbankan, dan kesehatan. Serangan siber seperti malware, ransomware, DDoS, dan phishing menjadi ancaman utama. Berdasarkan laporan dari Badan Siber dan Sandi Negara (BSSN) pada tahun 2023, terjadi peningkatan drastis dalam serangan siber, terutama dari ransomware dan DDoS yang merugikan sistem TI nasional.[1]

Data dari BSSN menunjukkan bahwa serangan ransomware naik 35% dan DDoS meningkat 22%[1]. pada tahun 2023 dibandingkan tahun sebelumnya. Sektor pemerintahan paling terdampak, diikuti oleh sektor perbankan dan kesehatan. Untuk mengatasi ancaman ini, diperlukan sistem keamanan yang kuat berbasis cybersecurity yang dapat mendeteksi dan merespons ancaman dengan cepat dan efektif.[2]

Penggunaan teknologi keamanan seperti SNORT IDS, Port Knocking, dan Artificial Intelligence (AI) telah diterapkan untuk deteksi ancaman siber. SNORT IDS efektif dalam mendeteksi malware dan ransomware, sementara AI meningkatkan deteksi ransomware. Port Knocking digunakan untuk meningkatkan keamanan akses, meskipun masih perlu peningkatan dalam mitigasi serangan DDoS.

Penelitian ini bertujuan merancang sistem keamanan jaringan yang menggabungkan teknologi-teknologi tersebut guna memberikan solusi mitigasi ancaman siber yang lebih efektif di Indonesia sesuai regulasi BSSN. Sistem ini diharapkan dapat meningkatkan deteksi dan respons terhadap serangan siber demi melindungi infrastruktur TI di Indonesia.

2. KAJIAN TEORITIS

2.1 Keamanan Jaringan (Network Security)

Keamanan jaringan merupakan praktik yang dilakukan untuk melindungi sistem komputer, perangkat, dan data dari ancaman baik yang berasal dari dalam maupun luar jaringan. Tujuan utama keamanan jaringan adalah untuk memastikan integritas, kerahasiaan, dan ketersediaan data, serta melindungi sumber daya jaringan dari ancaman yang dapat merusak atau mengakses data secara ilegal. Pentingnya perancangan sistem keamanan jaringan yang efektif sangat ditekankan dalam mencegah serangan siber yang dapat merugikan infrastruktur TI suatu organisasi atau negara[1].

Beberapa komponen krusial dalam keamanan jaringan termasuk firewall, Sistem Deteksi Intrusi (IDS), Sistem Pencegahan Intrusi (IPS), dan teknologi enkripsi. Keamanan jaringan yang efektif adalah yang mampu mendeteksi serta merespons ancaman dengan cepat, juga dapat meminimalisir potensi kerusakan pada sistem dan data yang telah ada.

2.2 Cybersecurity dan Perkembangannya

Keamanan Siber adalah upaya yang diambil untuk melindungi sistem komputer, data, dan jaringan dari ancaman di dunia maya. Menurut National Institute of Standards and Technology (NIST), keamanan siber mencakup berbagai teknik, praktik, dan kebijakan yang digunakan untuk melindungi informasi digital dari pencurian, kerusakan, atau gangguan. Di Indonesia, ancaman siber terhadap sektor-sektor krusial seperti pemerintahan, perbankan,

dan kesehatan, semakin meningkat. Berdasarkan laporan Badan Siber dan Sandi Negara (BSSN), serangan siber di Indonesia dapat menimbulkan kerugian finansial serta mengancam keamanan data pribadi maupun nasional[2].

Ancaman utama yang sering terjadi meliputi malware, ransomware, phishing, dan serangan DDoS (Distributed Denial of Service). Contohnya, ransomware dapat mengenkripsi data vital di sistem dan meminta tebusan untuk mendekripsinya, sedangkan serangan DDoS dapat membuat layanan atau situs web tidak dapat diakses oleh pengguna yang sah. Oleh karena itu, pengembangan sistem keamanan yang menggabungkan berbagai metode deteksi dan respons terhadap ancaman menjadi sangat penting untuk mengurangi risiko tersebut.

2.3 Intrusion Detection System IDN dan SNORT

Sistem Deteksi Intrusi (IDS) merupakan perangkat atau aplikasi yang didesain untuk mengenali aktivitas atau prilaku yang mencurigakan dalam jaringan yang dapat menandakan adanya ancaman potensial. IDS dapat dibagi menjadi dua jenis: IDS Berbasis Host (HIDS) dan IDS Berbasis Jaringan (NIDS). HIDS fokus pada pemantauan aktivitas di dalam sistem host, sementara NIDS memonitor lalu lintas jaringan untuk mendeteksi serangan yang melibatkan komunikasi antar sistem.

Salah satu IDS yang banyak dipakai adalah SNORT. SNORT ialah sistem deteksi intrusi yang berbasis jaringan yang bersifat open-source dan sangat terkenal di kalangan profesional keamanan siber. SNORT bekerja dengan menganalisis paket data yang mengalir dalam jaringan untuk memeriksa pola-pola serangan tertentu yang didasarkan pada tanda tangan yang telah ada. SNORT dapat mengenali berbagai jenis serangan, termasuk malware, DDoS, dan eksploitasi port. SNORT pun bisa dipasangkan dengan sistem pemrograman lain untuk meningkatkan kemampuannya dalam mendeteksi ancaman yang lebih kompleks dan canggih[3].

2.4 Port Knocking

Port Knocking ialah teknik keamanan jaringan yang diterapkan guna memastikan keamanan akses ke sistem atau jaringan dengan menyembunyikan port yang cuma bisa diakses lewat serangkaian "knocks" dalam pola yang tertentu. Metode ini menambah lapisan keamanan ekstra pada sistem dengan memanfaatkan protokol jaringan yang sudah ada. Secara praktis, port knocking dipakai untuk menjaga sistem dari akses tanpa izin dengan cara menantikan pola "knock" yang sah sebelum membuka port untuk akses lanjutan.

Port knocking beroperasi sebagai metode otentikasi tersembunyi yang amat efektif dalam menghadapi serangan brute-force atau metode lain yang berupaya menebak kredensial akses[4]. Pemanfaatan Port Knocking diharapkan bisa meningkatkan tingkat perlindungan pada jaringan, terutama untuk mengamankan server yang rentan terhadap serangan luar.

2.5 Kecerdasan Buatan (Artificial Intelligence) dalam Keamanan Siber

Kecerdasan Buatan (AI) dalam bidang keamanan cyber semakin banyak digunakan untuk meningkatkan kemampuan sistem dalam mendeteksi dan merespons ancaman secara otomatis. Teknologi ini memanfaatkan machine learning dan deep learning untuk menganalisis pola perilaku di dalam lalu lintas

jaringan serta mengidentifikasi potensi serangan berdasarkan data yang jauh lebih besar dan kompleks dibandingkan dengan yang biasanya ditangani oleh sistem berbasis tanda tangan.

Dalam beberapa penelitian, penggunaan AI dalam Sistem Deteksi Intrusi telah terbukti dapat meningkatkan tingkat deteksi ancaman, terutama untuk serangan zero-day yang sebelumnya belum pernah terdeteksi. Menurut penelitian yang dilakukan oleh Novica dkk. (2023), aplikasi AI dalam sistem IDS dapat meningkatkan akurasi dalam mendeteksi serangan ransomware dan malware hingga lebih dari 90%, angka yang jauh lebih tinggi dibandingkan dengan sistem konvensional yang hanya mengandalkan tanda tangan[5].

2.6 Regulasi Keamanan Siber di Indonesia

Di Indonesia, regulasi terkait keamanan siber dikeluarkan oleh **Badan Siber dan Sandi Negara (BSSN)**. Tugas BSSN adalah mengawasi dan melindungi infrastruktur TI nasional dari serangan siber. Demi menjaga keamanan di dunia maya, BSSN telah menerbitkan beragam kebijakan dan pedoman yang harus diikuti oleh instansi pemerintah, sektor swasta, dan masyarakat secara menyeluruh.

Regulasi utama yang mengatur keamanan siber di Indonesia termasuk **Peraturan Presiden No. 95 Tahun 2018** mengenai Sistem Pemerintahan Berbasis Elektronik (SPBE), yang menegaskan pentingnya perlindungan data pribadi dan penggunaan teknologi yang aman. BSSN juga telah mengembangkan berbagai inisiatif untuk meningkatkan kesadaran dan keterampilan dalam menghadapi ancaman siber yang terus berkembang.

3. METODE PENELITIAN

Penelitian ini menggunakan pendekatan analisis data sekunder, di mana informasi yang digunakan diperoleh dari jurnal ilmiah, artikel penelitian, dan laporan studi kasus yang relevan. Data sekunder ini mencakup hasil eksperimen dan simulasi yang telah dilakukan pada penelitian terdahulu tentang SDN, DPI, IPS, dan otomatisasi jaringan.

3.1 Pendekatan Penelitian

Penelitian ini memanfaatkan metode kualitatif yang difokuskan pada pengumpulan dan analisis *data sekunder*. Data yang dianalisis melibatkan laporan, publikasi, serta studi kasus yang relevan terkait ancaman siber di Indonesia dan sistem keamanan yang telah diterapkan. Tujuan penelitian ini adalah untuk menyajikan gambaran kondisi terkini terkait ancaman siber beserta upaya mitigasi yang telah dilakukan oleh sektor Teknologi Informasi di Indonesia.

3.2 Jenis Data

Penelitian ini hanya menggunakan data sekunder**,** yang terdiri dari berbagai jenis sumber informasi yang telah diterbitkan sebelumnya. Jenis data yang digunakan adalah

a. Dokumen tahunan dan survei yang dirilis oleh institusi terkait seperti Badan Siber dan Sandi Negara (BSSN)**,** AwanPintar.id, dan lembaga lainnya.
b. Informasi statistik yang meliputi jumlah serangan siber, jenis ancaman, serta dampak serangan siber terhadap infrastruktur TI di Indonesia.

c. Penelitian terbitan atau laporan teknis yang menguraikan berbagai metode keamanan jaringan yang diterapkan di Indonesia untuk mengatasi ancaman siber, seperti penggunaan Intrusion Detection Systems (IDS)**,** Port Knocking**,** dan kecerdasan buatan (AI).

3.3 Pengumpulan Data

Data yang digunakan dalam penelitian ini dikumpulkan melalui metode studi pustaka. Berikut adalah sumber-sumber utama yang digunakan:

a. Laporan BSSN**:** Informasi tentang tren ancaman siber dan evaluasi tindakan mitigasi yang dilakukan oleh pemerintah untuk melindungi infrastruktur TI di Indonesia.
b. Laporan AwanPintar.id: Data terkait ancaman digital yang mempengaruhi sektor-sektor kritis, termasuk industri perbankan, kesehatan, dan pemerintahan, beserta analisis kerentanannya.
c. Jurnal dan artikel ilmiah: Materi yang membicarakan teknologi keamanan jaringan dan sistem pertahanan siber yang relevan, mencakup implementasi metode IDS, Port Knocking, dan kecerdasan buatan dalam pendeteksian ancaman siber.

3.4 Analisis Data

Setelah mengumpulkan data sekunder, langkah selanjutnya adalah melakukan analisis kualitatif dengan tujuan, Mengidentifikasi tren ancaman siber yang terjadi di sektor Teknologi Informasi Indonesia dalam beberapa tahun terakhir, Menilai efektivitas pendekatan yang telah diterapkan oleh sektor TI dalam mengatasi ancaman siber tersebut,Menilai kelayakan regulasi yang ada, seperti kebijakan yang dikeluarkan oleh BSSN, terhadap upaya mitigasi yang dilakukan oleh sektor TI di Indonesia.

Data yang diperoleh dari laporan BSSN dan AwanPintar.id akan dianalisis untuk memahami, Jenis-jenis ancaman siber yang paling umum terjadi, Dampak ancaman siber terhadap sektor TI dan ekonomi nasional**,** Respon dan upay**a** mitigasi yang dilakukan oleh sektor TI, termasuk penggunaan teknologi dan prosedur keamanan.

3.5 Penyajian Data

Hasil analisis data sekunder akan disajikan dalam bentuk **tabel naratif** untuk memberikan gambaran yang jelas mengenai kondisi terkini ancaman siber dan upaya mitigasi yang dilakukan. Tabel yang relevan akan digunakan untuk memperkuat temuan penelitian.

3.6 Sumber Data

Data yang digunakan dalam penelitian ini merupakan data sekunder yang diperoleh dari sumber-sumber berikut:

a. Badan Siber dan Sandi Negara (BSSN)**:** Data mengenai ancaman siber dan upaya mitigasi yang dilakukan oleh BSSN seperti yang terdokumentasikan dalam laporan tahunan mereka. Laporan tersebut memberikan gambaran mengenai tren ancaman dan dampak serangan siber di Indonesia.
b. AwanPintar.id**:** Data ancaman digital yang terjadi di berbagai sektor Teknologi Informasi yang dipublikasikan oleh AwanPintar.id dalam laporan semesteran mereka.

c. Jurnal Teknologi dan Keamanan Jaringan**:** Publikasi yang mencakup penelitian dan studi kasus terkait dengan teknologi keamanan jaringan yang digunakan untuk mitigasi ancaman siber.

4. HASIL DAN PEMBAHASAN

Berdasarkan analisis data yang diperoleh dari laporan tahunan Badan Siber dan Sandi Negara (BSSN) 2023 dan laporan AwanPintar.id 2024, terdapat peningkatan signifikan dalam ancaman siber yang dihadapi oleh Indonesia. Ancaman-ancaman utama seperti malware, ransomware, dan serangan Distributed Denial of Service (DDoS) tercatat meningkat setiap tahunnya, terutama menyerang sektor-sektor penting seperti pemerintahan, perbankan, dan kesehatan. Laporan dari BSSN dan AwanPintar.id menunjukkan bahwa serangan malware dan ransomware menjadi yang paling umum, dengan dampak kerugian yang besar bagi sektor TI. Sementara itu, serangan DDoS yang mengarah pada penghentian layanan juga mengalami kenaikan signifikan, menekankan perlunya penguatan sistem keamanan untuk mencegah gangguan operasional dan menjaga integritas data.

Dalam upaya mitigasi, sejumlah teknologi keamanan telah diterapkan di sektor TI Indonesia, termasuk penggunaan Intrusion Detection Systems (IDS) seperti SNORT, metode Port Knocking, dan penerapan Kecerdasan Buatan (AI) untuk mendeteksi ancaman berbasis perilaku. IDS seperti SNORT terbukti efektif dalam mendeteksi intrusi dan anomali pada jaringan, terutama di sektor pemerintahan dan perbankan. Penggunaan teknologi Port Knocking juga umum meskipun dengan tingkat efektivitas yang lebih rendah dibandingkan SNORT, khususnya di sektor dengan kebutuhan keamanan tinggi dan infrastruktur kompleks seperti sektor pemerintahan. Sementara penggunaan AI menunjukkan efektivitas yang tinggi dalam mendeteksi ancaman berbasis perilaku, dengan pengurangan false positives dan peningkatan respons terhadap ancaman. Penerapan AI terbukti paling efektif di sektor perbankan dan kesehatan yang membutuhkan perlindungan data yang ketat.Meskipun telah dilakukan berbagai upaya mitigasi, Indonesia masih menghadapi sejumlah tantangan besar dalam implementasi keamanan siber yang optimal. Salah satu tantangan utama adalah kekurangan sumber daya manusia yang terlatih dalam bidang keamanan siber. Banyak sektor TI di Indonesia masih kekurangan tenaga ahli yang memiliki kompetensi untuk mengelola ancaman siber yang semakin kompleks. Selain itu, sektor-sektor TI Indonesia masih sangat bergantung pada teknologi keamanan asing, yang menimbulkan potensi risiko, terutama dalam hal pemeliharaan dan integrasi sistem. Ketergantungan pada teknologi asing ini menunjukkan perlunya pendekatan yang lebih mandiri dalam hal pengembangan dan penggunaan solusi keamanan yang berbasis teknologi domestik. Keterbatasan infrastruktur juga menjadi masalah, terutama di sektor-sektor yang memerlukan tingkat perlindungan tinggi terhadap data sensitif. Beberapa sektor TI masih belum memiliki infrastruktur yang memadai untuk menghadapi ancaman yang lebih besar dan lebih canggih.

Berdasarkan temuan-temuan ini, terdapat beberapa rekomendasi yang dapat diajukan untuk meningkatkan sistem keamanan jaringan di Indonesia. Pertama, diperlukan investasi lebih besar dalam pelatihan sumber daya manusia di bidang keamanan siber untuk meningkatkan kemampuan sektor TI dalam menghadapi ancaman siber. Kedua, pemanfaatan teknologi terbaru seperti AI dan machine learning harus diperluas, agar ancaman dapat terdeteksi lebih cepat dan respons terhadap serangan bisa lebih efektif. Ketiga, perlu penguatan regulasi dan kebijakan

yang mendorong sektor TI untuk menggunakan solusi keamanan yang lebih baik serta kolaborasi yang lebih erat antara sektor publik dan sektor privat dalam menghadapi ancaman siber. Hal ini menjadi sangat penting untuk meningkatkan ketahanan nasional terhadap serangan siber.

Dengan demikian, walaupun terdapat kemajuan dalam penerapan sistem keamanan siber di Indonesia, tantangan dan kebutuhan akan peningkatan infrastruktur dan sumber daya manusia masih perlu mendapatkan perhatian lebih, agar dapat menciptakan sistem keamanan yang lebih tangguh dan mampu melindungi sektor TI dari ancaman yang terus berkembang.

5. KESIMPULAN DAN SARAN

Penelitian ini menyimpulkan bahwa ancaman siber di Indonesia seperti malware, ransomware, dan serangan DDoS terus meningkat secara signifikan. Sektor-sektor seperti pemerintahan, perbankan, dan kesehatan menjadi yang paling rentan. Teknologi keamanan jaringan seperti Sistem Deteksi Intrusi (IDS) SNORT, Port Knocking, dan penerapan Kecerdasan Buatan (AI) terbukti efektif dalam mendeteksi dan menanggapi ancaman tersebut. Meskipun demikian, Indonesia masih menghadapi tantangan besar, terutama terkait keterbatasan sumber daya manusia yang terlatih di bidang keamanan siber dan ketergantungan pada teknologi asing. Untuk mengatasi masalah ini, perlu ditingkatkan kapasitas sumber daya manusia dan infrastruktur keamanan di sektor Teknologi Informasi (TI) Indonesia.

Sebagai tindak lanjut, penelitian ini menyarankan adanya pelatihan yang lebih intensif guna meningkatkan keterampilan tenaga ahli di bidang keamanan siber. Selain itu, pemanfaatan teknologi canggih seperti AI dan machine learning perlu diperluas untuk mempercepat deteksi dan respons terhadap ancaman. Penguatan infrastruktur keamanan jaringan juga menjadi hal penting, dengan fokus utama pada pengembangan solusi teknologi dalam negeri. Terakhir, kolaborasi antara sektor publik dan privat harus ditingkatkan guna membangun ekosistem keamanan yang lebih solid dan tahan banting terhadap ancaman siber yang semakin kompleks.

DAFTAR REFERENSI

[1]. Badan Siber dan Sandi Negara, "*Laporan Tahunan Monitoring Keamanan Siber Tahun 2023*," Badan Siber dan Sandi Negara (BSSN), 2023. https://www.bssn.go.id/

[2]. AwanPintar.id, "*Laporan Ancaman Digital Semester 1 Tahun 2024*" AwanPintar.id, 2024. https://www.awanpintar.id/

[3]. Winrou Wesley Purba and Rissal Efendi, *"Perancangan dan Analisis Sistem Keamanan Jaringan Komputer Menggunakan SNORT," AITI Jurnal Teknologi Informasi*, vol. 10, no. 3, pp. 155-166, 2021. https://ejournal.uksw.edu/aiti/article/view/3939

[4]. Nugroho A.s and Khaediar B.a and Rifki D.K, *"Perancangan dan Implementasi Sistem Keamanan Jaringan dengan Metode Port Knockin," Jurnal Teknologi Komputer dan Sistem Informasi*, vol. 15, no. 4, pp. 98-110, 2022. https://janitra.org/index.php/home/article/view/156

[5]. Novica H.S and Deci Irmayani and Mila N.S.H, "*Mengoptimalkan Keamanan Jaringan: Memanfaatkan Kecerdasan Buatan untuk Meningkatkan Deteksi dan Respons Ancaman," Jurnal Sistem Informasi dan Komputer Terapan*, vol. 17, no. 2, pp. 45-58, 2023. https://ejournal.sisfokomtek.org/index.php/jikom/article/view/3582

[6]. Milleano J.A and Wiwin S., *"Perancangan Sistem Keamanan Jaringan Berbasis Hierarchical Network Design*,**"** *Jurnal Teknologi Informasi dan Komunikasi Eksplorasi*, vol. 12, no. 1, pp. 23-35, 2022. https://ejournal.uksw.edu/itexplore/article/view/7588

[7]. Sutamo, *"Analisa dan Perancangan Sistem Keamanan Jaringan Menggunakan Teknik ACL*,**"** *Jurnal Ilmiah Informatika*, vol. 19, no. 3, pp. 199-210, 2023. https://eprints.ums.ac.id/27312/

[8]. Putu R and Putu S and Ichsan W.**,** *"Sistem Keamanan Jaringan Komputer dan Data dengan Menggunakan Metode Port Knocking," Jurnal Sistem Informasi Keamanan Teknologi Informasi*, vol. 14, no. 4, pp. 33-47, 2023. https://infoteks.org/journals/index.php/jsikti/article/view/12

[9]. Muhammad Hafidz Maulana, *"Analisis Sistem Keamanan Jaringan Komputer Menggunakan Metode Snort IDS untuk Pencegahan Penyusupan Jaringan*,**"** *Jurnal Teknik Informatika dan Sistem Informasi*, vol. 21, no. 5, pp. 76-88, 2023. https://elibrary.bsi.ac.id/skripsi/B21720230081I01/analisis-sistem-keamanan-jaringan-komputer-menggunakan-metode-snort-ids-untuk-pencegahan-penyusupan-jaringan

[10]. Fathurrahman Dali,*"Sistem Keamanan Jaringan Menggunakan Cisco AnyConnect dengan Metode Network Access Manager," Jurnal Ilmu Teknologi Komputer dan Sistem Informasi*, vol. 18, no. 3, pp. 102-115, 2023 https://publikasi.mercubuana.ac.id/index.php/jitkom/article/view/5090