TIN: Terapan Informatika Nusantara
Vol 6, No 7, December 2025, page 1240-1249
ISSN 2722-7987 (Media Online)
Website https://ejurnal.seminar-id.com/index.php/tin
DOI 10.47065/tin.v6i7.8899

Perancangan Basis Pengetahuan pada Sistem Pakar Identifikasi Jenis Serangan Keamanan Jaringan dengan Metode Rule-Based System

Nico Bustanul Anshary

Fakultas Teknik dan Ilmu Komputer, Program Studi Teknik Informatika, Universitas Indraprasta PGRI, Jakarta Selatan, Indonesia
Email: nico.anshary@gmail.com

Abstrak–Ancaman keamanan jaringan terus berkembang seiring dengan meningkatnya kompleksitas dan skala infrastruktur jaringan. Oleh karena itu, diperlukan suatu model analisis ancaman yang mampu merepresentasikan pola serangan secara terstruktur dan sistematis. Penelitian ini bertujuan untuk merancang basis pengetahuan analisis ancaman keamanan jaringan menggunakan metode rule-based reasoning dengan mekanisme inferensi forward chaining. Pengetahuan direpresentasikan dalam bentuk aturan IF–THEN yang disusun berdasarkan karakteristik serangan serta dipetakan ke dalam kerangka kerja MITRE ATT&CK. Basis pengetahuan yang dikembangkan mencakup sepuluh jenis ancaman utama, meliputi serangan terhadap ketersediaan layanan, akses tidak sah, eksekusi kode berbahaya, pergerakan lateral, hingga aktivitas pengintaian jaringan. Validasi basis pengetahuan dilakukan melalui pemeriksaan kesesuaian teoritis, konsistensi logika aturan, serta pengujian menggunakan skenario pengujian konseptual. Hasil pengujian menunjukkan bahwa seluruh aturan mampu menghasilkan inferensi yang tepat dan konsisten sesuai dengan kondisi ancaman yang diberikan, tanpa ditemukan konflik maupun ambiguitas antaraturan. Hasil penelitian menunjukkan bahwa pendekatan rule-based dengan forward chaining efektif digunakan untuk memodelkan dan menganalisis ancaman keamanan jaringan pada tingkat konseptual. Model basis pengetahuan yang dihasilkan diharapkan dapat menjadi dasar bagi pengembangan sistem analisis atau deteksi ancaman keamanan jaringan pada penelitian selanjutnya.

Kata kunci: Keamanan Jaringan; Basis Pengetahuan; *Rule-Based*; *Forward Chaining*; MITRE ATT&CK

Abstract–Network security threats continue to evolve along with the increasing complexity and scale of network infrastructures. Therefore, a threat analysis model that can represent attack patterns in a structured and systematic manner is required. This study aims to design a knowledge base for network security threat analysis using a rule-based reasoning approach with a forward chaining inference mechanism. Knowledge is represented in the form of IF–THEN rules, which are constructed based on attack characteristics and mapped to the MITRE ATT&CK framework. The developed knowledge base covers ten major types of threats, including attacks on service availability, unauthorized access, malicious code execution, lateral movement, and reconnaissance activities. Knowledge base validation was conducted through theoretical conformity assessment, logical consistency analysis of the rules, and testing using conceptual test scenarios. The results show that all rules produce accurate and consistent inferences according to the given threat conditions, with no conflicts or ambiguities identified. The findings indicate that the rule-based approach with forward chaining is effective for modeling and analyzing network security threats at a conceptual level. The resulting knowledge base model can serve as a foundation for the development of network security threat analysis or detection systems in future research.

Keywords: Network Security; Knowledge Base; Rule-Based; Forward Chaining; MITRE ATT&CK

1. PENDAHULUAN

Perkembangan teknologi informasi yang begitu pesat telah membawa perubahan besar dalam berbagai aspek kehidupan (Setiawan, 2018), mulai dari dunia bisnis, pendidikan, pemerintahan, hingga aktivitas sehari-hari masyarakat. Konektivitas jaringan komputer dan internet memungkinkan pertukaran informasi berlangsung dengan cepat dan efisien (Aulia et al., 2023), namun di sisi lain juga memunculkan tantangan serius terkait keamanan data dan sistem (Asnawi et al., 2025). Serangan keamanan jaringan atau cyber attack menjadi salah satu ancaman utama yang harus diwaspadai (Laode et al., 2024). Berbagai bentuk serangan seperti *malware*, *phishing*, *ransomware*, hingga *denial of service* dapat menyebabkan kerugian besar, baik dari sisi finansial maupun kerahasiaan informasi (Simatangkir et al., 2025).

Masalah yang sering muncul dalam konteks ini adalah ketidakmampuan banyak organisasi atau individu untuk secara cepat mengenali jenis serangan yang terjadi pada jaringan mereka. Keterlambatan dalam mendeteksi pola serangan dapat berakibat fatal, mulai dari pencurian data, kebocoran informasi, hingga terhentinya layanan yang bersifat vital (Karimi & Yusuf, 2025). Kondisi ini menunjukkan perlunya suatu pendekatan yang mampu membantu dalam mengidentifikasi serangan berdasarkan gejala-gejala sistem yang tampak sehingga langkah penanganan dapat segera dilakukan.

Meskipun Indonesia telah memiliki beberapa undang-undang yang mengatur kejahatan *cyber*, seperti UU ITE dan UU PDP, namun masih banyak kelemahan dalam sistem keamanan siber di Indonesia (Ilaina & Nugraha, 2025). Beberapa faktor yang menyebabkan kelemahan tersebut antara lain kurangnya kesadaran masyarakat tentang keamanan siber, kurangnya sumber daya manusia yang ahli di bidang keamanan siber, dan kurangnya dukungan teknologi yang memadai (Setiawan et al., 2023).

Tujuan dari penelitian ini adalah untuk melakukan analisis mendalam terhadap berbagai jenis serangan keamanan jaringan yang umum terjadi serta mengidentifikasi gejala-gejala sistem yang dapat dijadikan indikator awal terjadinya serangan. Berdasarkan hasil analisis tersebut, penelitian ini bertujuan menyusun basis pengetahuan dalam bentuk aturan *rule-based* menggunakan struktur IF-THEN yang menggambarkan hubungan logis antara gejala dan jenis serangan secara sistematis. Metode yang digunakan adalah *Rule-Based System.* Pemilihan metode ini didasarkan pada kemampuannya dalam merepresentasikan pengetahuan pakar melalui aturan-aturan yang sederhana namun jelas (Subali & Fatichah, 2019), sehingga dapat mempermudah proses penalaran ketika sistem harus menentukan jenis serangan yang

TIN: Terapan Informatika Nusantara
Vol 6, No 7, December 2025, page 1240-1249
ISSN 2722-7987 (Media Online)
Website https://ejurnal.seminar-id.com/index.php/tin
DOI 10.47065/tin.v6i7.8899

sedang terjadi. Sistem pakar yang dibangun diharapkan dapat memberikan diagnosis awal yang membantu administrator jaringan dalam mengambil keputusan yang tepat dan cepat ketika menghadapi potensi serangan siber.

Landasan teori yang mendukung penelitian ini mencakup konsep keamanan jaringan yang menekankan pentingnya menjaga kerahasiaan, integritas, dan ketersediaan data dari berbagai ancaman. Selain itu, teori mengenai sistem pakar sebagai bagian dari kecerdasan buatan yang menggunakan basis pengetahuan untuk memecahkan masalah spesifik juga menjadi dasar penting (Sajida et al., 2024). Metode Rule Based System digunakan sebagai mekanisme inferensi yang bekerja melalui aturan-aturan *if-then* untuk menarik kesimpulan dari gejala yang terdeteksi (Yamin & Sulindawaty, 2024). Di samping itu, pemahaman mengenai gejala sistem akibat serangan siber, seperti peningkatan trafik jaringan yang tidak wajar, aktivitas login mencurigakan, atau penurunan kinerja sistem, turut menjadi elemen penting yang mendasari perancangan sistem ini.

Terdapat beberapa penelitian terdahulu yang serupa dengan penelitian yang dilakukan. Penelitian pertama adalah penelitian yang dilakukan oleh Mubarok & Romli (2025) yang berjudul implementasi Metode Rule Based dalam Mendeteksi Serangan Brute Force pada *Owncloud*. Pada penelitian ini penulis akan melakukan analisis forensik jaringan (Network Forensic) menggunakam tools seperti Wireshark dan Snort pada server owncloud yang diserang menggunakan serangan brute force attack terhadap sistem keamanan server owncloud, dengan aturan-aturan (rule-based) pada sistem server owncloud. Penerapan metode rule based pada penelitian yang dilakukan melibatkan aturan penggunaan dan skenario yang sudah ditentukan sebelumnya untuk mengidentifikasi pola serangan yang mencurigakan. Hal ini termasuk memeriksa pola aktivitas login, seperti mengetahui jumlah upaya login yang gagal selama periode waktu tertentu dari IP yang sama. Metode *rule based* menggunakan aturan (*rule*) sebagai representasi pengetahuan yang diterapkan dalam sistem.

Penelitian kedua dilakukan oleh Haryono & Zulianda (2021) yang berjudul sistem pendeteksian serangan jaringan Local Area Network (LAN) menggunakan algoritma naive bayes. Penelitian ini dilatarbelakangi Ada banyak sekali gangguan atau serangan jaringan komputer, salah satu diantaranya adalah Spoofing, DdoS, DNS Poisoning, Trojan House, Sniffer, SQL Injection, Cross Site Scripting, Phising, Malware, Worm, sementara disisi lain tidak ada sistem deteksi yang mumpuni untuk mendiagnosa jenis serangan jaringan komputer. Hasil penelitian ini adalah sebuah sistem deteksi berbasis web untuk deteksi serangan jaringan LAN. Dari hasil penelitian dibuktikan bahwa Algoritma Naive Bayes dapat melakukan pendeteksian serangan jaringan LAN yang dapat membantu user untuk mengtahui jenis serangan dan cara mengatasinya.

Penelitian ketiga dilakukan oleh Esterlin et al., (2024) yang berjudul Deteksi Serangan dalam Jaringan Komputer dengan Algoritma Pohon Keputusan C4.5. Penelitian ini memberikan kontribusi penting dalam pengembangan sistem deteksi serangan yang lebih efektif dan dapat diandalkan dalam konteks jaringan komputer. Dengan memanfaatkan kekuatan algoritma pohon keputusan C4.5, kami berharap dapat membantu meningkatkan keamanan sistem informasi dan melindungi infrastruktur jaringan dari ancaman cyber yang semakin kompleks dan berkembang.

Berdasarkan penelitian-penelitian terdahulu tersebut, dapat disimpulkan bahwa metode yang digunakan dalam deteksi serangan jaringan sangat beragam, mulai dari pendekatan berbasis aturan hingga algoritma pembelajaran mesin seperti Naive Bayes dan C4.5. Pendekatan berbasis pembelajaran mesin memiliki keunggulan dalam pengolahan data berskala besar, namun memerlukan data latih yang cukup dan menghasilkan proses pengambilan keputusan yang tidak selalu mudah dipahami oleh pengguna. Oleh karena itu, penelitian ini memilih menerapkan metode Rule-Based System karena mampu memberikan hasil deteksi yang jelas dan mudah ditelusuri melalui aturan IF–THEN yang terdefinisi. Berbeda dengan penelitian terdahulu yang fokus pada implementasi sistem deteksi atau evaluasi algoritma, penelitian ini menekankan pada implementasi metode rule-based yang disertai dengan perancangan mockup aplikasi sebagai gambaran antarmuka sistem pakar. Mockup ini bertujuan untuk menunjukkan alur penggunaan sistem serta interaksi pengguna dengan hasil deteksi serangan, sehingga dapat menjadi dasar pengembangan aplikasi sistem pakar deteksi serangan keamanan jaringan secara lebih lengkap pada tahap selanjutnya.

2. METODOLOGI PENELITIAN

Penelitian ini merupakan penelitian deskriptif yang menggunakan pendekatan rekayasa pengetahuan (*knowledge engineering*). Pendekatan ini dipilih karena mampu merepresentasikan pengetahuan pakar ke dalam suatu sistem secara terstruktur. Fokus utama penelitian adalah pada perancangan basis pengetahuan dalam sistem pakar. Sistem pakar tersebut digunakan untuk mengidentifikasi jenis serangan keamanan jaringan. Identifikasi dilakukan berdasarkan gejala atau indikasi yang muncul pada sistem jaringan. Gejala-gejala tersebut dikumpulkan dari pengetahuan pakar dan literatur terkait keamanan jaringan. Pengetahuan yang diperoleh kemudian direpresentasikan dalam bentuk aturan (*rules*). Metode penalaran yang digunakan dalam sistem ini adalah *rule-based reasoning*. Setiap aturan menghubungkan gejala tertentu ddengan jenis serangan keamanan jaringan. Dengan demikian, sistem yang dibangun diharapkan mampu memberikan hasil identifikasi serangan secara sistematis
dan akurat.

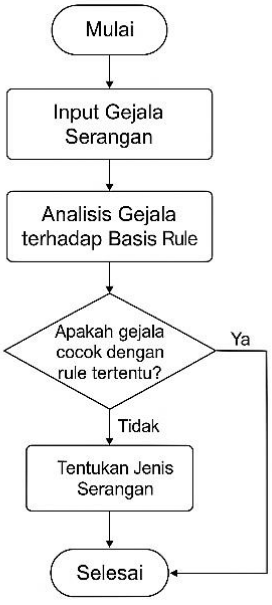
Gambar 1 adalah alur penelitian yang dilaksanakan pada penelitian ini. gambar tersebut menggambarkan alur kegiatan penelitian mulai dari tahap awal hingga selesai. Tahap pertama dimulai dari identifikasi masalah untuk menentukan kebutuhan dan ruang lingkup penelitian. Identifikasi permasalahan penelitian salah satu langkah yang paling penting dalam penelitian (Nasution, 2021). Tahap kedua dilakukan studi literatur. Studi literatur dilakukan

TIN: Terapan Informatika Nusantara
Vol 6, No 7, December 2025, page 1240-1249
ISSN 2722-7987 (Media Online)
Website https://ejurnal.seminar-id.com/index.php/tin
DOI 10.47065/tin.v6i7.8899

dengan mencari referensi yang relevan dengan sebuah topik penelitian (Qorimah & Sutama, 2022). Tahap keempat adalah pengumpulan data jenis serangan dan jenis gejala sebagai dasar dalam menyusun basis aturan. Selain itu juga pengumpulan data tentang rekomendasi penanganan yang sesuai dengan masing-masing serangan. Tahap kelima adalah analisis menggunakan metode Rule-Based, Setelah dilakukan analisis dengan metode Rule-based, dilakukan validasi terhadap basis pengetahuan, Tahap terakhir adalah perancangan prototype sebagai implementasi dari solusi yang diusulkan. Setelah seluruh tahapan selesai, penelitian ditutup dengan proses dokumentasi dan penyelesaian akhir.

Gambar 1. Alur Penelitian

Aturan rule-base system dapat direpresentasikan dengan ‘Jika x adalah A, maka yadalah B’ dan bagian-jika dari aturan ‘x adalah A’disebut anteseden atau premis, sedangkan bagian-bagian selanjutnya dari aturan 'y adalah B' disebutkonsekuensi atau kesimpulan (Rakhmawati et al., 2018). Pada jenis penalaran ini, bagian kondisi harus terpenuhi terlebih dahulu agar bagian hasil dapat dicapai (Farajollahi & Baradaran, 2024). Pendekatan Rule-Based System" telah membuktikan efektivitas penerapan basis pengetahuan dalam menghasilkan diagnosis (Syifa et al., 2025).



Gambar 1. Flowchart

Gambar 2 adalah flowchart dari setiap rule dimana tahapan dimulai dengan penginputan gejala, di analisis gejala terhadap basis rule, apabila gejala cocok dengan rule tertentu maka selesai, apabila gejala tidak cocok dengan rule tertentu maka tentukan jenis serangan.

3. HASIL DAN PEMBAHASAN

3.1 Jenis Serangan

Basis pengetahuan pada penelitian ini disusun menggunakan pendekatan *rule-based* yang merepresentasikan pola ancaman keamanan jaringan berdasarkan atribut confidentiality, integrity, dan availability. Aturan-aturan (R1–R10) dirumuskan melalui studi literatur sistematis serta mengacu pada standar dan kerangka kerja keamanan siber yang telah diakui secara luas, seperti MITRE ATT&CK (Strom et al., 2020) dan penelitian terdahulu terkait deteksi serangan berbasis log jaringan. Dengan demikian, basis aturan yang dibangun tidak bersifat arbitrer, melainkan memiliki landasan teoritis dan praktis yang jelas. Dalam proses analisis ancaman, mekanisme inferensi yang digunakan adalah forward chaining. Mekanisme ini bekerja dengan menjadikan fakta-fakta awal yang berasal dari kejadian pada log jaringan sebagai pemicu inferensi. Setiap fakta dicocokkan dengan kondisi pada aturan IF–THEN.

TIN: Terapan Informatika Nusantara
Vol 6, No 7, December 2025, page 1240-1249
ISSN 2722-7987 (Media Online)
Website https://ejurnal.seminar-id.com/index.php/tin
DOI 10.47065/tin.v6i7.8899

Tabel 1. Jenis Serangan

Kode Rule	Jenis Serangan	Tingkat Keparahan
R1	Distributed Denial of Service (DDoS)	High
R2	Brute Force Attack	High
R3	Command and Control (C2) / Botnet	High
R4	Malware / Backdoor / Cryptominer	High
R5	Ransomware	Critical
R6	Data Exfiltration	High
R7	SQL Injection	Medium
R8	Web Shell / Remote Code Execution	High
R9	Lateral Movement (SMB / Pass-the-Hash)	High
R10	Port Scanning / Reconnaissance	Low

Tabel 1 berisi berisi daftar jenis serangan siber beserta deskripsi singkat mengenai cara kerja dan tujuan masing-masing serangan. Mulai dari serangan yang berfokus pada gangguan layanan seperti DDoS, hingga serangan yang menargetkan pencurian data, eksploitasi aplikasi, dan pengambilalihan sistem. Beberapa serangan dilakukan secara langsung, seperti *brute force atau SQL injection*, sementara lainnya bersifat tersembunyi dan berkelanjutan seperti *malware, ransomware*, dan *lateral movement.*

3.2 Daftar Gejala

Untuk masing-masing jenis serangan, penulis menyusun daftar gejala yang dapat diambil dari log jaringan, log aplikasi, dan artefak host. Format gejala disiapkan agar mudah dipetakan ke kondisi boolean atau threshold numerik (mis. true/false atau > threshold). Gejala umum yang digunakan (digunakan sebagai building block across rules) adalah sebagai berikut :

Tabel 2. Daftar Gejala

Kode Gejala	Deskripsi Gejala
G1	Volume trafik masuk meningkat signifikan
G2	Jumlah request serentak dari banyak sumber sangat tinggi
G3	Layanan mengalami penurunan performa atau tidak responsif
G4	Percobaan login gagal melebihi ambang batas
G5	Percobaan login terjadi dalam rentang waktu singkat
G6	Percobaan login berasal dari satu atau banyak alamat IP
G7	Host melakukan koneksi keluar secara periodik
G8	Koneksi menuju alamat eksternal yang sama
G9	Pola komunikasi tidak sesuai aktivitas normal
G10	File atau executable tidak dikenal dijalankan
G11	Penggunaan CPU atau resource sistem meningkat abnormal
G12	Proses berjalan secara persisten
G13	Terjadi enkripsi massal file dalam waktu singkat
G14	Ekstensi file berubah secara tidak normal
G15	Terdapat pesan atau indikasi tuntutan tebusan
G16	Pengiriman data keluar jaringan secara signifikan
G17	Tujuan transfer tidak sah atau tidak dikenal
G18	Data yang dikirim bersifat sensitif
G19	Input aplikasi web mengandung pola sintaks SQL berbahaya
G20	Terjadi error database atau query tidak normal
G21	Akses dilakukan melalui parameter input pengguna
G22	File skrip tidak sah diunggah ke web server
G23	File dapat dieksekusi
G24	Memungkinkan eksekusi perintah jarak jauh
G25	Terjadi akses ke banyak host internal
G26	Menggunakan kredensial yang sama
G27	Pola autentikasi tidak sesuai perilaku normal
G28	Satu host melakukan koneksi ke banyak port
G29	Koneksi dilakukan dalam waktu singkat
G30	Tidak menghasilkan sesi layanan normal

Tabel 2 memuat berbagai gejala teknis yang dapat menjadi indikator adanya serangan siber dalam sistem atau jaringan. Gejala tersebut mencakup lonjakan trafik anomali, aktivitas login mencurigakan, proses asing, perubahan file,

TIN: Terapan Informatika Nusantara
Vol 6, No 7, December 2025, page 1240-1249
ISSN 2722-7987 (Media Online)
Website https://ejurnal.seminar-id.com/index.php/tin
DOI 10.47065/tin.v6i7.8899

hingga koneksi jaringan yang tidak biasa. Dengan mengenali pola-pola ini, administrator dapat mendeteksi ancaman lebih cepat sebelum terjadi kerusakan atau kompromi sistem yang lebih luas.

3.3 Basis Pengetahuan *(Rule Based)*

Basis pengetahuan direpresentasikan dalam bentuk aturan IF–THEN yang menggambarkan hubungan antara indikator kejadian keamanan jaringan dan jenis ancaman yang diidentifikasi. Aturan-aturan ini digunakan dalam mekanisme inferensi forward chaining, di mana fakta awal yang diperoleh dari log jaringan dievaluasi terhadap kondisi aturan untuk menghasilkan kesimpulan berupa jenis serangan dan tingkat keparahannya.

1. R1 – Distributed Denial of Service (DDoS)
   IF volume_trafik_masuk meningkat signifikan AND jumlah_request_serentak dari banyak sumber sangat tinggi AND layanan mengalami penurunan performa atau tidak responsif
   THEN
   serangan = Distributed Denial of Service (DDoS)
   severity = High
2. R2 – Brute Force Attack
   IF percobaan_login_gagal > threshold AND terjadi dalam rentang waktu singkat AND berasal dari satu atau banyak alamat IP
   THEN
   serangan = Brute Force Attack
   severity = High
3. R3 – Command and Control (C2) / Botnet
   IF host melakukan koneksi keluar secara periodik AND tujuan koneksi ke alamat eksternal yang sama AND pola komunikasi tidak sesuai dengan aktivitas normal
   THEN
   serangan = Command and Control (C2) / Botnet
   severity = High
4. R4 – Malware / Backdoor / Cryptominer
   IF file atau executable tidak dikenal dijalankan AND penggunaan CPU atau resource sistem meningkat abnormal AND proses berjalan secara persisten
   THEN
   serangan = Malware / Backdoor / Cryptominer
   severity = High
5. R5 – Ransomware
   IF terjadi enkripsi massal file dalam waktu singkat AND ekstensi file berubah secara tidak normal AND terdapat pesan atau indikasi tuntutan tebusan
   THEN
   serangan = Ransomware
   severity = Critical
6. R6 – Data Exfiltration
   IF terjadi pengiriman data keluar jaringan secara signifikan AND tujuan transfer tidak sah atau tidak dikenal AND data bersifat sensitif
   THEN
   serangan = Data Exfiltration
   severity = High
7. R7 – SQL Injection
   IF input aplikasi web mengandung pola sintaks SQL berbahaya AND terjadi error database atau query tidak normal AND akses dilakukan melalui parameter input pengguna
   THEN
   serangan = SQL Injection
   severity = Medium
8. R8 – Web Shell / Remote Code Execution
   IF file skrip tidak sah diunggah ke web server AND file dapat dieksekusi AND memungkinkan perintah jarak jauh dijalankan
   THEN
   serangan = Web Shell / Remote Code Execution
   severity = High
9. R9 – Lateral Movement (SMB / Pass-the-Hash)
   IF terjadi akses ke banyak host internal AND menggunakan kredensial yang sama AND pola autentikasi tidak sesuai perilaku normal
   THEN
   serangan = Lateral Movement
   severity = High

TIN: Terapan Informatika Nusantara
Vol 6, No 7, December 2025, page 1240-1249
ISSN 2722-7987 (Media Online)
Website https://ejurnal.seminar-id.com/index.php/tin
DOI 10.47065/tin.v6i7.8899

10. R10 – Port Scanning / Reconnaissance
    IF satu host melakukan koneksi ke banyak port AND dalam waktu singkat AND tidak menghasilkan sesi layanan normal
    THEN
    serangan = Port Scanning / Reconnaissance
    severity = Low

3.4 Rekomendasi penangangan

Tabel 3. Rekomendasi penanganan

No	Jenis Serangan	Rekomendasi Penanganan
1	*Distributed Denial of Service (DDoS)*	Rate-limit & WAF/CDN.
2	*Brute Force Attack*	Block IP, enforce MFA.
3	*Command & Control (C2) / Botnet*	Isolate host, block domain.
4	*Malware / Backdoor / Cryptominer*	Isolate & scan.
5	*Ransomware*	Isolate, restore backup.
6	*Data Exfiltration*	Blokir tujuan & audit.
7	*SQL Injection*	Block payload & patch.
8	*Web Shell / Remote Code Execution*	Remove webshell & harden upload.
9	*Lateral Movement (SMB / Pass-the-Hash)*	Segment network & reset creds.
10	*Port Scanning / Reconnaissance*	Block IP & monitor.

Tabel 3 berisi daftar/rekomendasi penanganan yang sesuai untuk masing-masing kasus. Setiap baris menunjukkan satu tipe serangan, seperti *DDoS, Brute Force, Botnet, Ransomware*, hingga *Port Scanning*, yang umum terjadi pada sistem informasi modern. Kolom pertama menampilkan nomor urut, kolom kedua menjelaskan jenis serangan, dan kolom ketiga memberikan tindakan mitigasi yang direkomendasikan berdasarkan karakteristik serangan tersebut. Tabel ini digunakan untuk mempermudah identifikasi ancaman dan menentukan langkah respons yang tepat dalam proses analisis insiden keamanan siber.

3.5 Validasi Basis Pengetahuan

Pengujian basis pengetahuan dilakukan menggunakan skenario pengujian konseptual untuk mengevaluasi ketepatan inferensi aturan IF–THEN yang dirancang. Setiap skenario merepresentasikan kondisi ancaman keamanan jaringan yang umum terjadi dan disusun berdasarkan indikator-indikator yang sesuai dengan definisi serangan pada literatur dan kerangka kerja MITRE ATT&CK. Pada setiap skenario, sekumpulan kondisi awal diberikan sebagai fakta masukan, kemudian dievaluasi terhadap aturan dalam basis pengetahuan menggunakan mekanisme inferensi forward chaining. Hasil inferensi yang dihasilkan dibandingkan dengan jenis serangan yang diharapkan pada masing-masing skenario. Pengujian ini bertujuan untuk memastikan bahwa setiap aturan menghasilkan kesimpulan yang tepat ketika kondisi yang didefinisikan terpenuhi.

Tabel 4. Skenario Pengujian Basis Pengetahuan

Skenario	Kondisi yang Diberikan	Aturan Terpicu	Hasil yang Diharapkan
S1	Lonjakan trafik sangat tinggi dari banyak IP, layanan tidak responsif	R1	DDoS
S2	Login gagal berulang > threshold dalam waktu singkat	R2	Brute Force Attack
S3	Host melakukan koneksi keluar periodik ke IP yang sama	R3	Command & Control
S4	Proses tidak dikenal berjalan, CPU tinggi	R4	Malware / Cryptominer
S5	Enkripsi massal file dalam waktu singkat	R5	Ransomware
S6	Transfer data besar ke alamat eksternal tidak dikenal	R6	Data Exfiltration
S7	Input web mengandung sintaks SQL abnormal	R7	SQL Injection
S8	File skrip berbahaya dapat dieksekusi di web server	R8	Web Shell / RCE
S9	Akses banyak host internal dengan kredensial sama	R9	Lateral Movement
S10	Satu host memindai banyak port dalam waktu singkat	R10	Reconnaissance

Hasil pengujian menunjukkan bahwa seluruh skenario pengujian memicu aturan yang sesuai dan menghasilkan jenis serangan yang konsisten dengan tujuan perancangan basis pengetahuan. Tidak ditemukan kondisi di mana aturan menghasilkan kesimpulan yang keliru atau ambigu. Dengan demikian, basis pengetahuan dinilai mampu merepresentasikan pola ancaman keamanan jaringan secara logis dan konsisten pada tingkat konseptual.

3.6 Protoype Sistem Pakar

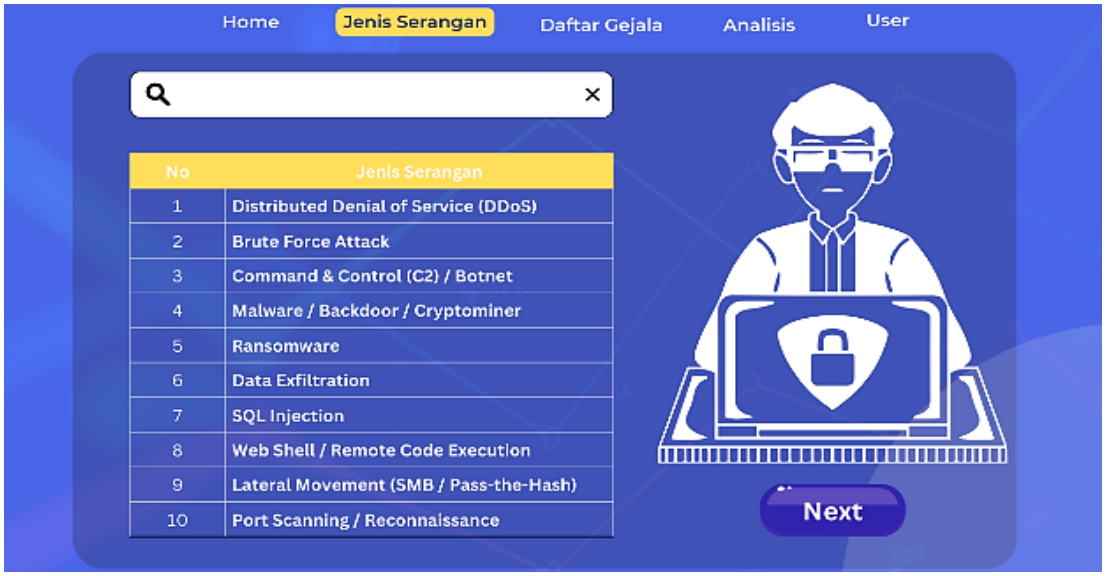
Perancangan antarmuka aplikasi merupakan salah satu aspek penting dalam pengembangan sebuah sistem. Antarmuka berfungsi sebagai media interaksi antara pengguna dan sistem sehingga harus dirancang dengan baik. Antarmuka yang

TIN: Terapan Informatika Nusantara
Vol 6, No 7, December 2025, page 1240-1249
ISSN 2722-7987 (Media Online)
Website https://ejurnal.seminar-id.com/index.php/tin
DOI 10.47065/tin.v6i7.8899

efektif mampu membantu pengguna dalam memahami fungsi dan alur kerja sistem. Selain itu, perancangan antarmuka perlu memperhatikan kemudahan penggunaan dan kejelasan penyajian informasi. Tata letak, navigasi, serta konsistensi tampilan menjadi faktor yang memengaruhi kenyamanan pengguna. Antarmuka yang baik juga dapat mengurangi kesalahan dalam penggunaan sistem. Oleh karena itu, perancangan antarmuka aplikasi dilakukan secara terencana agar sistem dapat digunakan secara optimal dan sesuai dengan kebutuhan pengguna. Dalam proses perancangannya, kebutuhan dan karakteristik pengguna menjadi salah satu pertimbangan utama. Antarmuka perlu dirancang agar dapat digunakan secara efisien tanpa memerlukan pembelajaran yang rumit. Selain itu, antarmuka yang responsif dapat meningkatkan pengalaman pengguna dalam mengoperasikan sistem. Perancangan antarmuka juga harus mendukung alur kerja sistem secara keseluruhan.

Gambar 2. Prototype Beranda

Gambar 3 berisi prototype untuk halaman beranda. Halaman ini menampilkan antarmuka utama dari sistem pakar yang berfokus pada identifikasi serangan keamanan jaringan. Bagian atas menyediakan menu navigasi seperti Home, Jenis Serangan, Daftar Gejala, Analisis, dan User untuk memudahkan akses fitur. sistem ini memiliki fungsi utama melakukan identifikasi serangan berdasarkan data atau gejala yang diberikan.



Gambar 3. Prototype Halaman Jenis Serangan

Gambar 4 adalah prototype halaman jenis serangan. Halaman ini menampilkan daftar jenis serangan keamanan jaringan yang tersedia dalam sistem pakar. Di bagian atas terdapat bilah pencarian untuk memudahkan pengguna menelusuri jenis serangan secara lebih spesifik. Tabel berisi nomor urut dan nama serangan yang tersusun secara terstruktur. Di sisi kanan terdapat ilustrasi dan tombol "Next" untuk melanjutkan ke daftar serangan selanjutnya.

TIN: Terapan Informatika Nusantara
Vol 6, No 7, December 2025, page 1240-1249
ISSN 2722-7987 (Media Online)
Website https://ejurnal.seminar-id.com/index.php/tin
DOI 10.47065/tin.v6i7.8899

Gambar 4. Prototype Halaman Daftar Gejala

Gambar 5 adalah prototype halaman daftar gejala. Halaman ini menampilkan daftar gejala yang dapat digunakan sebagai indikator dalam proses identifikasi serangan keamanan jaringan. Pada bagian atas terdapat kolom pencarian yang memungkinkan pengguna mencari gejala tertentu secara lebih cepat. Tabel berisi nomor urut dan deskripsi gejala yang tersusun secara sistematis.

Gambar 5. Prototype Halaman analisa

Gambar 6 adalah prototype halaman analisa, dimana user akan diberikan pertanyaan tertentu yang akan mengarahkan kepada kesimpulan untuk mendapatkan diagnosa jenis serangan jaringan yang di alami. Setiap pertanyaan user akan diminta untuk memilih Ya jika kondisi terpenuhi, dan memilih tidak jika kondisi tidak terpenuhi.

Gambar 6. Protoype Halaman hasil analisa

Gambar 7 adalah prototype halaman hasil diagnosa. Setelah melewati serangkaian pertanyaan yang mengarahkan kepada kesimpulan, Sistem akan memberikan konklusi jenis serangan jaringan jenis apa yang dialami oleh user.

TIN: Terapan Informatika Nusantara
Vol 6, No 7, December 2025, page 1240-1249
ISSN 2722-7987 (Media Online)
Website https://ejurnal.seminar-id.com/index.php/tin
DOI 10.47065/tin.v6i7.8899

Gambar 7. Prototype Halaman User

Gambar 8 adalah prototype halaman user. Tampilan antarmuka ini menunjukkan halaman user dengan struktur navigasi yang sederhana dan mudah dipahami. Menu di bagian atas berisi akses menuju fitur utama seperti Home**,** Jenis Serangan**,** Daftar Gejala**,** Analisis**,** dan profil User. Bagian kiri menampilkan ilustrasi avatar pengguna, sedangkan area kosong di sisi kanan berfungsi sebagai ruang konten dinamis tentang profil singkat user.

4. KESIMPULAN

Penelitian ini menerapkan metode rule-based reasoning dengan mekanisme inferensi forward chaining dalam perancangan basis pengetahuan untuk analisis ancaman keamanan jaringan. Pengetahuan direpresentasikan dalam bentuk aturan IF–THEN yang menghubungkan indikator ancaman dengan jenis serangan berdasarkan kerangka kerja MITRE ATT&CK. Hasil pengujian basis pengetahuan menggunakan skenario pengujian konseptual menunjukkan bahwa seluruh aturan mampu menghasilkan inferensi yang sesuai dengan kondisi ancaman yang diberikan. Setiap skenario pengujian memicu aturan yang tepat dan tidak ditemukan konflik maupun ambiguitas antaraturan. Hal ini menunjukkan bahwa basis pengetahuan yang dirancang konsisten secara logika dan valid secara konseptual dalam merepresentasikan pola ancaman keamanan jaringan. Dengan demikian, pendekatan rule-based dengan forward chaining yang digunakan pada penelitian ini terbukti efektif sebagai model representasi dan analisis ancaman pada tingkat konseptual, serta dapat dijadikan fondasi awal dalam pengembangan sistem analisis ancaman keamanan jaringan. Penelitian selanjutnya disarankan untuk mengimplementasikan basis pengetahuan yang telah dirancang ke dalam sistem deteksi ancaman yang bersifat operasional agar dapat diuji menggunakan data lalu lintas jaringan nyata. Selain itu, metode inferensi dapat dikembangkan lebih lanjut dengan mengombinasikan pendekatan rule-based dan metode probabilistik atau pembelajaran mesin untuk meningkatkan adaptabilitas terhadap pola serangan yang dinamis. Pengembangan basis pengetahuan juga dapat diperluas dengan menambahkan jenis ancaman baru serta memperbarui aturan secara berkala mengikuti perkembangan taktik dan teknik serangan pada kerangka kerja MITRE ATT&CK, sehingga sistem tetap relevan dan responsif terhadap evolusi ancaman keamanan jaringan. Selain itu, antarmuka sistem dapat dikembangkan lebih lanjut untuk meningkatkan pengalaman pengguna, terutama dalam penyajian hasil analisis dan rekomendasi keamanan.

REFERENCES

Asnawi, M. F., Fitriyanto, N., & Pamoengkas, M. A. (2025). Tinjauan Pustaka Sistematis Tentang Teknologi Keamanan Data : Tren Dan Tantangan. *TECHNOMEDIA : Informatics and Computer Science*, *2*(2), 72–79.

Aulia, B. W., Rizki, M., Prindiyana, P., & Surgana, S. (2023). Peran Krusial Jaringan Komputer dan Basis Data dalam Era Digital. *JUSTINFO | Jurnal Sistem Informasi Dan Teknologi Informasi*, *1*(1), 9–20. https://doi.org/10.33197/justinfo.vol1.iss1.2023.1253

Esterlin, E., Sihombing, V., & Juledi, A. P. (2024). Deteksi Serangan dalam Jaringan Komputer dengan Algoritma Pohon Keputusan C4.5. *Jurnal Ilmu Komputer Dan Sistem Informasi (JIKOMSI)*, *7*(1), 322–327. https://doi.org/https://doi.org/10.55338/jikomsi.v7i1.3087

Farajollahi, M., & Baradaran, V. (2024). Expert system application in law : A review of research and applications. *International Journal of Nonlinear Analysis and Applications*, *15*(July 2023), 107–114. https://doi.org/https://doi.org/10.22075/ijnaa.2023.31260.4596

Haryono, D., & Zulianda, Y. (2021). Sistem Pendeteksian Serangan Jaringan Local Area Network (Lan) Menggunakan Algoritma Naive Bayes. *JOISIE Journal Of Information System And Informatics Engineering*, *5*(1), 1–8. https://doi.org/https://doi.org/10.35145/joisie.v5i1.949

Ilaina, A. S. A., & Nugraha, F. (2025). terjadi, mulai dari pencurian data sampai dengan peretasan. *Triwikrama: Jurnal Multidisiplin Ilmu Sosial*, *8*(6), 1–15. https://doi.org/https://doi.org/10.9963/fb6a9g13

Karimi, B. I., & Yusuf, A. R. (2025). Kebocoran Data dan Distributed Denial of Service (DDoS) dalam Cloud Computing: Systematic Literature Review. *Integrative Perspectives of Social and Science Journal*, *2*(3), 3871–3879.


TIN: Terapan Informatika Nusantara
Vol 6, No 7, December 2025, page 1240-1249
ISSN 2722-7987 (Media Online)
Website https://ejurnal.seminar-id.com/index.php/tin
DOI 10.47065/tin.v6i7.8899

Laode, I. U., Rizal, A. S., & Isnawaty, I. (2024). Deteksi Serangan Siber Pada Jaringan Komputer Menggunakan Metode Random Forest. *JATI (Jurnal Mahasiswa Teknik Informatika)*, *8*(3), 2787–2793. https://doi.org/10.36040/jati.v8i3.8891

Mubarok, K., & Romli, M. A. (2025). Implementation of Rule Based Method in Detecting Brute Force Attacks on Owncloud Implementasi Metode Rule Based dalam Mendeteksi Serangan Brute Force pada Owncloud. *MALCOM: Indonesian Journal of Machine Learning and Computer Science*, *5*(January), 159–167. https://doi.org/https://doi.org/10.57152/malcom.v5i1.1701

Nasution, A. R. S. (2021). Identifikasi Permasalahan Penelitian. *ALACRITY : Journal Of Education*, *1*(2), 13–19. https://doi.org/https://doi.org/10.52121/alacrity.v1i2.21

Qorimah, E. N., & Sutama, S. (2022). Studi Literatur: Media Augmented Reality (AR) Terhadap Hasil Belajar Kognitif. *JURNALBASICEDU*, *6*(2), 2055–2060. https://doi.org/https://doi.org/10.31004/basicedu.v6i2.2348

Rakhmawati, N. A., Septa, A., Budi, S., Atletiko, F. J., Maulida, K., Ramadhani, F., & Handayani, S. F. (2018). Penentuan Prioritas Pengambilan Pesanan Barang Oleh Angkutan Kota Dengan Metode Rule-Based System. *Jurnal Sistem Informasi Bisnis*, *02*(1), 195–202. https://doi.org/10.21456/vol8iss2pp195-202

Sajida, M., Yuhandri, Y., & Nurcahyo, G. W. (2024). Perancangan Sistem Pakar Dengan Metode Forward Chaining dan Certainty Factor Untuk Mendeteksi Penyakit Kelinci. *Jurnal KomtekInfo*, *11*, 98–105. https://doi.org/10.35134/komtekinfo.v11i3.546

Setiawan, D. (2018). Dampak Perkembangan Teknologi Informasi dan Komunikasi Terhadap Budaya Impact of Information Technology Development and Communication on. *Jurnal Simbolika*, *4*(1), 62–72. https://doi.org/10.31289/simbollika.v4i1.1474

Setiawan, D., Pratama, M. C., & Arisandi, D. (2023). Implementasi Sistem Keamanan Jaringan Menggunakan Rule-Based Ids Pada Pt Netkrida Tuah Cakrawala. *JOISIE Journal Of Information System And Informatics Engineering*, *7*(2), 381–389. https://doi.org/https://doi.org/10.35145/joisie.v7i2.4014

Simatangkir, D. W. E. S., Afifah, E. F. N., & Faliha, N. S. (2025). Keamanan Siber dalam Perbankan Serta Tantangan dan Solusi di Era Digital. *Jurnal Multidisiplin Ilmu Akademik*, *2*(1), 33–42. https://doi.org/10.1484/m.tt-eb.4.2017009

Strom, B. E., Miller, D. P., Nickels, K. C., Pennington, A. G., & Thomas, C. B. (2020). MITRE ATT & CK ® : Design and Philosophy. *The MITRE Corporation*, *July 2018*, 1–46.

Subali, M. A. P., & Fatichah, C. (2019). Kombinasi Metode Rule-Based dan N-Gram Stemming untuk Mengenali Stemmer Bahasa Bali. *Jurnal Teknologi Informasi Dan Ilmu Komputer*, *6*(2), 219–228. https://doi.org/10.25126/jtiik.2019621105

Syifa, P., Safwandi, S., & Fitri, Z. (2025). Sistem pakar diagnosis penyakit paru menggunakan metode convolutional neural network dan rule based system 1) 1,2,3). *RABIT : Jurnal Teknologi Dan Sistem Informasi Univrab*, *10*(2), 1380–1392. https://doi.org/https://doi.org/10.36341/rabit.v10i2.6548

Yamin, M., & Sulindawaty, S. (2024). Implementasi Sistem Pakar Deteksi Dini Penyakit Demam Berdarah Dengue Menggunakan Metode Rule Based Reasoning (Rumah Sakit Umum Bandung). *JOURNAL DATA SCIENCE PENUSA (JDSP)*, *1*(1), 1–8.