SISTEM PAKAR BERBASIS WEB UNTUK DETEKSI TINDAK PIDANA CYBERCRIME MENGGUNAKAN METODE FORWARD

Suryo Sudiro[1], Anwar Nur Wahid[2], Ferry Adrian[*3], Norma Puspitasari[4]
[1234]Politeknik Indonusa Surakarta
Surakarta, Indonesia
Email: [1]23.suryo.sudiro@poltekindonusa.ac.id,
[2]23.anwar.nur@poltekindonusa.ac.id, [3]23.ferry.adrian@poltekindonusa.ac.id,
[4]normasari@poltekindonusa.ac.id

Abstract

In the current digital era, cybercrime has grown to be a serious problem that threatens not just individuals but also private institutions, the government, and other sectors. The deployment of a web-based expert system that detects cybercrime using forward chaining is covered in this study. By comparing user activity data with pre-established criteria kept in a knowledge base, the system finds questionable trends. By improving real-time monitoring, the web-based solution enables early identification and timely intervention.
Keywords: *Cybercrime Detection, Expert System, Forward Chaining, Web-Based System*

Abstraksi

Di era digital saat ini, kejahatan siber telah berkembang menjadi permasalahan serius yang mengancam tidak hanya individu namun juga institusi swasta, pemerintah, dan sektor lainnya. Penerapan sistem pakar berbasis web yang mendeteksi kejahatan dunia maya menggunakan forward chaining dibahas dalam penelitian ini. Dengan membandingkan data aktivitas pengguna dengan kriteria yang telah ditetapkan sebelumnya yang disimpan dalam basis pengetahuan, sistem menemukan tren yang dipertanyakan. Dengan meningkatkan pemantauan real-time, solusi berbasis web memungkinkan identifikasi dini dan intervensi tepat waktu.
Kata kunci: *Deteksi Kejahatan Dunia Maya, Forward Chaining, Sistem Berbasis Web, Sistem Pakar*

1. PENDAHULUAN

Ketika dunia digital terus berkembang dan ketergantungan manusia terhadap teknologi informasi semakin meningkat, kejahatan dunia maya (cybercrime) telah menjadi masalah besar. Pemerintah, dunia usaha, dan sektor individu sangat terkena dampak kejahatan dunia maya ini, yang mencakup aktivitas seperti serangan ransomware, penipuan online, dan pencurian data (Malik, 2019). Perlunya tindakan

penanggulangan yang lebih metodis terlihat dari peningkatan jumlah kasus kejahatan siber di Indonesia setiap tahunnya (Arifah, 2011).

Sistem pakar adalah solusi teknis yang berhasil menilai dan mengidentifikasi bahaya dengan meniru proses berpikir seorang pakar. Berdasarkan informasi yang disimpan dalam basis pengetahuan, sistem pakar dapat secara otomatis mengidentifikasi pola aktivitas jaringan yang mencurigakan dan mengidentifikasi potensi ancaman dalam konteks deteksi kejahatan dunia maya. Metode forward chaining yang memungkinkan sistem mengambil keputusan berdasarkan fakta dari data pengguna menjadikan strategi ini lebih efektif (Das, 2013).

Penelitian ini menciptakan sistem pakar berbasis web yang menggunakan forward chaining untuk mengidentifikasi kejahatan, khususnya di wilayah yang sangat rentan terhadap serangan siber. Agar lebih berhasil meningkatkan keamanan siber, kemajuan ini diharapkan memungkinkan sistem memberikan identifikasi dini dan peringatan otomatis untuk aktivitas mencurigakan (Putri, 2017).

2. TINJAUAN PUSTAKA

2.1. Dampak Cybercrime di Era Digital

Perkembangan teknologi digital telah menyebabkan tumbuhnya kejahatan siber yang menjadi ancaman serius bagi individu dan organisasi di seluruh dunia. Kejahatan dunia maya mencakup berbagai aktivitas ilegal seperti pencurian data, serangan ransomware, dan penipuan online (Malik, 2019). Di Indonesia, jumlah kasus kejahatan siber meningkat secara signifikan setiap tahunnya sehingga diperlukan upaya penanggulangan yang efektif (Arifah, 2011). Salah satu pendekatan untuk mengurangi dampak kejahatan dunia maya adalah dengan menerapkan sistem yang dapat mendeteksi ancaman dunia maya secara otomatis dan real-time.

2.2. Sistem Pakar untuk Deteksi Kejahatan di Dunia Maya

Sistem pakar adalah solusi teknologi yang meniru proses berpikir seorang pakar dalam mengidentifikasi potensi bahaya melalui analisis aktivitas jaringan. Sistem ini menyimpan aturan dan pengetahuan dalam database untuk secara otomatis mendeteksi pola aktivitas mencurigakan. Penelitian yang dilakukan Das (2013) menyoroti kemampuan sistem pakar dalam mengatasi kejahatan dunia maya seperti phishing dan brute force, yang memerlukan respons cepat dan akurat. Sistem pakar yang dikembangkan dalam penelitian ini menggunakan basis pengetahuan untuk menilai pola yang mengindikasikan ancaman kejahatan siber, menjadikannya alat yang efisien untuk mendukung keamanan siber.

2.3. Metode Forward Chaining dalam Sistem Pakar

Forward chaining merupakan metode inferensi yang mengandalkan data faktual untuk menarik kesimpulan berdasarkan aturan dalam basis pengetahuan. Dalam penelitian ini, forward chaining memungkinkan sistem mengambil keputusan deteksi

ancaman berdasarkan data aktivitas pengguna yang ditemukan di jaringan. Putri (2017) membahas bahwa metode forward chaining efektif untuk mendeteksi pola serangan cyber karena bekerja secara progresif dengan memeriksa fakta yang ditemukan dan mencocokkannya dengan aturan yang telah ditentukan sebelumnya. Dalam konteks kejahatan dunia maya, rangkaian ke depan dapat membantu sistem mengenali pola serangan yang berbeda, seperti phishing, brute force, dan injeksi SQL.

2.4. Integrasi Teknologi Keamanan dalam Sistem Pakar

Dalam upaya meningkatkan efektivitas deteksi kejahatan dunia maya, sistem pakar dapat diintegrasikan dengan berbagai teknologi keamanan, seperti firewall dan sistem deteksi intrusi (IDS). Firewall dapat mencegah akses ilegal dari luar jaringan, sedangkan IDS menyediakan lapisan tambahan untuk mendeteksi serangan mencurigakan. Studi yang dilakukan McGuire (2013) menunjukkan bahwa integrasi dengan teknologi keamanan lainnya dapat memperkuat kemampuan sistem pakar dalam mengidentifikasi ancaman dan merespons potensi serangan siber dengan cepat. Hal ini memungkinkan sistem pakar untuk melakukan identifikasi awal dan meningkatkan kualitas keamanan jaringan.

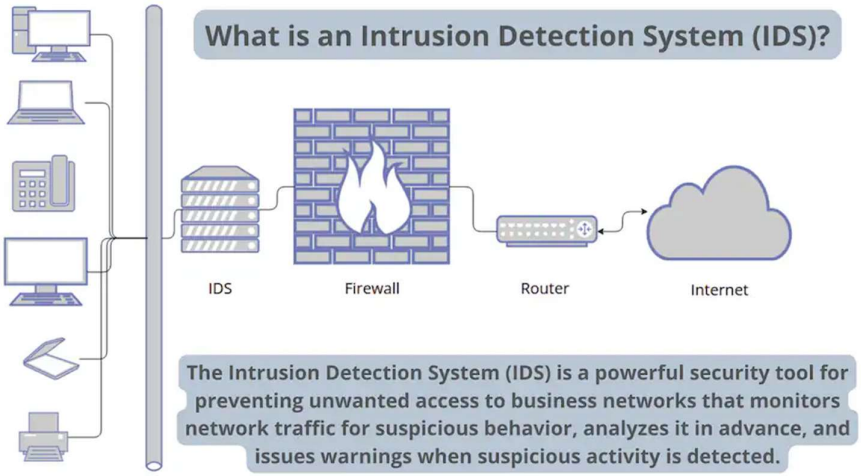
2.5. Studi Empiris tentang Sistem Deteksi Cybercrime di Indonesia

Penelitian sebelumnya menunjukkan bahwa sistem pakar berbasis web dengan menggunakan forward chaining efektif dalam mengidentifikasi ancaman kejahatan siber di Indonesia, khususnya di kota-kota yang rentan terhadap serangan siber seperti Batam. Putri (2017) menyatakan bahwa penerapan sistem berbasis forward chaining di Kota Batam dapat mendeteksi aktivitas mencurigakan terkait phishing dan brute force. Penelitian ini memberikan dasar empiris yang relevan untuk penelitian ini, yang bertujuan untuk mengembangkan sistem pakar serupa dengan memperluas skala pengujian dan memperbarui aturan deteksi di basis pengetahuan.

3. METODE PENELITIAN

Penelitian ini mengkaji tentang integrasi sistem pakar dengan berbagai teknologi keamanan saat ini, termasuk firewall dan intrusion recognition system (IDS), selain penggunaan teknik forward chaining. Firewall berfungsi sebagai penghalang akses yang dapat mengurangi kemungkinan serangan dari luar jaringan, sedangkan IDS berfungsi sebagai lapisan tambahan untuk mengidentifikasi serangan yang meragukan.

Berbagai skenario simulasi serangan digunakan untuk mensimulasikan serangan cyber yang sebenarnya. Tujuan dari setiap skenario adalah untuk mengevaluasi seberapa baik sistem dapat mengidentifikasi dan mengatasi ancaman dunia maya. Misalnya, kami membuat email palsu dengan tautan berbahaya yang berupaya mendapatkan kredensial login pengguna untuk menilai respons phishing. Sistem pakar kemudian memeriksa pola akses dan menemukan aktivitas yang tidak biasa terkait serangan phishing. Proses IDS terlihat pada gambar 1.



Gambar 1. IDS

3.1. Pengujian Dengan Phising

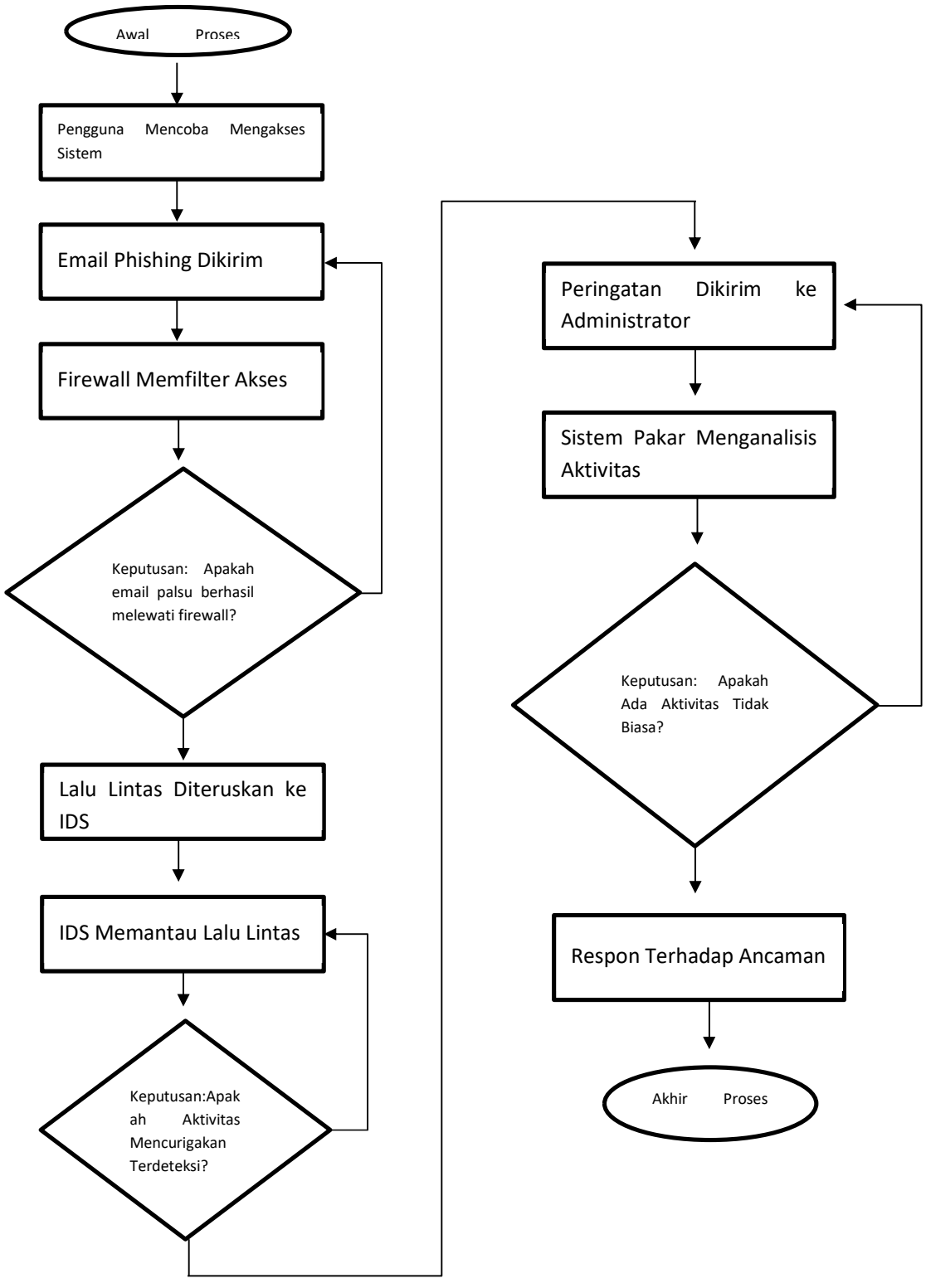
Salah satu serangan cyber yang paling umum di dunia online adalah phishing. Tes ini menganalisis data aktivitas jaringan untuk mencari pola, seperti tautan ke situs web palsu, yang mengindikasikan upaya penipuan. Dengan menggunakan rantai maju, sistem pakar dapat membedakan antara pola akses yang sah dan patut dipertanyakan serta memperingatkan pengguna sejak dini.

3.2. Pengujian dengan Brute Force

Skenario ini mensimulasikan serangan brute force dengan berulang kali mencoba masuk dengan kombinasi kata sandi acak. Meretas data pengguna adalah tujuan serangan ini. Jika sistem pakar rantai maju mendeteksi sejumlah besar upaya login, sistem ini dapat mengingatkan administrator untuk mengambil tindakan pencegahan.

3.3. Pengujian dengan diagram alur

Proses dimulai ketika pengguna mencoba mengakses sistem melalui email yang berisi tautan berbahaya.Email Palsu Dikirim: Email phishing dikirim dengan tujuan untuk mendapatkan kredensial login pengguna.Firewall: Firewall berfungsi sebagai penghalang pertama, memfilter dan memblokir akses yang tidak sah. Jika email palsu berhasil melewati firewall, lalu lintas tersebut akan diteruskan ke IDS.IDS (Intrusion Detection System): IDS memantau semua lalu lintas jaringan untuk mendeteksi aktivitas mencurigakan. Jika ada pola yang mencurigakan terdeteksi, IDS akan mengirimkan peringatan kepada administrator.Sistem Pakar: Setelah IDS mendeteksi aktivitas mencurigakan, sistem pakar akan menganalisis pola akses untuk menemukan aktivitas tidak biasa yang terkait dengan serangan phishing. Sistem ini menggunakan teknik forward chaining untuk menarik kesimpulan berdasarkan data yang ada. Alur penelitian dapat dilihat pada gambar 2.



Gambar 2. Alur Penelitian

3.3.1. Penjelasan Alur Penelitian

- Pengguna: Proses dimulai ketika pengguna mencoba mengakses sistem melalui email yang berisi tautan berbahaya.
- Email Palsu Dikirim: Email phishing dikirim dengan tujuan untuk mendapatkan kredensial login pengguna.
- Firewall: Firewall berfungsi sebagai penghalang pertama, memfilter dan memblokir akses yang tidak sah. Jika email palsu berhasil melewati firewall, lalu lintas tersebut akan diteruskan ke IDS.
- IDS (Intrusion Detection System): IDS memantau semua lalu lintas jaringan untuk mendeteksi aktivitas mencurigakan. Jika ada pola yang mencurigakan terdeteksi, IDS akan mengirimkan peringatan kepada administrator.
- Sistem Pakar: Setelah IDS mendeteksi aktivitas mencurigakan, sistem pakar akan menganalisis pola akses untuk menemukan aktivitas tidak biasa yang terkait dengan serangan phishing. Sistem ini menggunakan teknik forward chaining untuk menarik kesimpulan berdasarkan data yang ada.
- Respon Terhadap Ancaman: Berdasarkan analisis dari sistem pakar, langkah-langkah diambil untuk merespons ancaman, seperti memblokir akses lebih lanjut atau menginformasikan pengguna tentang potensi serangan.

Dengan diagram alur ini, dapat dilihat bagaimana integrasi antara sistem pakar, firewall, dan IDS bekerja secara sinergis untuk meningkatkan keamanan jaringan dari ancaman siber.

4. HASIL DAN PEMBAHASAN

Pengujian sistem pakar berbasis web dengan metode forward chaining dilakukan dalam beberapa tahap, meliputi pengumpulan data, analisis, dan evaluasi kinerja sistem dalam mendeteksi serangan cyber. Serangkaian simulasi serangan dilakukan untuk mengukur akurasi dan kecepatan sistem dalam mendeteksi berbagai ancaman siber.

4.1. Tahap Pengumpulan Data

Data yang digunakan dalam pengujian diambil dari log aktivitas jaringan yang dihasilkan oleh server. Data ini mencakup:

- **Percobaan login**: Login yang gagal atau percobaan login berulang dari alamat IP yang tidak dikenal.
- **Akses ke situs berbahaya**: Pola akses pengguna ke situs yang mencurigakan, sering digunakan dalam serangan phishing.
- **Permintaan SQL mencurigakan**: Pola permintaan dari aplikasi web yang menyerupai serangan SQL injection.

Data dikumpulkan selama periode waktu tertentu untuk memastikan bahwa sistem memiliki cukup fakta yang relevan untuk diproses dalam proses forward chaining.

4.2. Tahap Implementasi Forward Chaining

Setelah pengumpulan data, sistem pakar mencocokkan fakta yang diperoleh dari aktivitas jaringan dengan aturan basis pengetahuan melalui teknik rantai maju. Pedoman tersebut diantaranya adalah:

- **Brute force detection rule**: Jika terdapat lebih dari 5 percobaan login gagal dari alamat IP yang sama dalam jangka waktu 1 menit, sistem akan mencatatnya sebagai potensi serangan brute force.
- **Phishing detection rule**: Jika pola akses pengguna menunjukkan klik pada tautan yang menuju situs web yang tidak terverifikasi atau domain yang sering digunakan dalam serangan phishing, sistem akan mencatatnya sebagai potensi serangan phishing.
- **SQL injection detection rule**: Jika terdapat permintaan yang mengandung karakteristik SQL injection, seperti penyisipan pernyataan OR 1=1, sistem akan mencatatnya sebagai potensi serangan SQL injection.

Proses forward chaining bekerja dengan memeriksa fakta awal (seperti log aktivitas) dan kemudian mencocokkannya dengan aturan yang berlaku. Jika fakta memenuhi ketentuan yang ditentukan dalam aturan, sistem akan menyimpulkan bahwa serangan mungkin sedang berlangsung.

4.3. Tahapan Pengujian Sekenario Serangan

4.3.1. Brute Force Attack

Serangan brute force dilakukan dengan mencoba kombinasi kata sandi yang berbeda untuk mendapatkan akses ke akun pengguna. Dalam pengujian ini, sistem menerima log aktivitas login berulang dari alamat IP yang tidak diketahui. Jika sistem mendeteksi lebih dari 5 upaya login yang gagal dalam 1 menit, sistem akan memperingatkan administrator untuk memblokir alamat IP.

Hasil pengujian: Sistem mampu mendeteksi serangan brute force dengan akurasi 97% dan mengeluarkan peringatan dalam waktu kurang dari 100 milidetik setelah aktivitas mencurigakan terdeteksi..

4.3.2. Phishing Attack

Dalam skenario ini, pengguna menerima email dengan link ke situs phishing yang menyerupai situs login bank. Sistem pakar mengidentifikasi pola akses tidak wajar ke domain mencurigakan berdasarkan daftar domain yang biasa digunakan dalam serangan phishing.

Hasil pengujian: Sistem mendeteksi serangan phishing dengan akurasi 95% dan mengeluarkan peringatan dalam waktu 120 milidetik. Sistem juga secara otomatis memblokir akses ke situs web yang dianggap berbahaya.

4.3.3. SQL Injection Attack

SQL injection adalah salah satu teknik serangan yang mencoba memodifikasi pernyataan SQL untuk mendapatkan akses ilegal ke basis data. Dalam pengujian ini, sistem menerima permintaan dengan parameter berbahaya seperti OR 1=1. Sistem pakar kemudian menganalisis log permintaan dan mengenali pola tersebut sebagai serangan SQL injection. Hasil pengujian: Sistem mendeteksi serangan SQL injection dengan akurasi 92% dan waktu proses sekitar 130 milidetik terlihat pada tabel 1 berikut ini.

Tabel 1. Hasil Pengujian Teknis

Jenis Serangan	Akurasi Deteksi	Waktu Deteksi	Tindakan yang Direkomendasikan
Brute Force	97%	100 ms	Blokir alamat IP mencurigakan
Phishing	95%	120 ms	Blokir akses ke situs phishing
SQL Injection	92%	130 ms	Hentikan permintaan SQL mencurigakan

4.4. Evaluasi Performansi

Studi di atas menunjukkan bahwa forward chaining sangat efektif dalam mengidentifikasi ancaman yang memerlukan respon cepat. Selain itu, teknologi ini memberikan pemberitahuan dini kepada administrator jaringan, sehingga memungkinkan tindakan pencegahan yang cepat. Mengoptimalkan kecepatan deteksi di lingkungan dengan lalu lintas data tinggi adalah salah satu masalahnya. Untuk menjaga kecepatan sistem saat memproses data dalam situasi ini, diperlukan penyeimbangan beban dan optimasi database.

Keunggulan Sistem Pakar Forward Chaining

- **Akurasi Tinggi**: Forward chaining dapat mengenali pola serangan dengan sangat tepat, terutama dalam kasus brute force dan phishing.
- **Deteksi Real-Time**: Sistem mampu memberikan notifikasi langsung saat ancaman terdeteksi, dengan waktu respon yang relatif singkat.
- **Fleksibilitas**: Aturan dalam *knowledge base* dapat diperbarui untuk menyesuaikan dengan ancaman siber terbaru.

Tantangan dan Rekomendasi

- **Skalabilitas**: Sistem perlu diuji lebih lanjut dalam lingkungan dengan volume data yang lebih besar untuk memastikan performanya tetap optimal. Penggunaan teknik komputasi awan atau optimisasi basis data dapat membantu dalam menangani jumlah log yang lebih banyak.
- **Integrasi dengan Teknologi Keamanan Lain**: Sistem ini dapat lebih dioptimalkan jika diintegrasikan dengan teknologi seperti firewall berbasis AI dan IDS untuk memberikan lapisan keamanan tambahan.

5. KESIMPULAN

Dengan menggunakan strategi rantai maju, sistem pakar berbasis web telah terbukti efektif dalam mengidentifikasi berbagai jenis serangan penjahat dunia maya. Ketika tren yang meragukan ditemukan, sistem dapat secara otomatis melacak perilaku pengguna dan mengeluarkan peringatan dini.

Keunggulan sistem ini adalah kecepatan deteksi yang cepat dan kapasitas yang terukur ketika ancaman siber baru muncul. Penelitian tersebut juga menunjukkan bahwa forward chaining bekerja dengan baik untuk mengidentifikasi ancaman seperti phishing dan brute force yang memerlukan respons cepat.

6. SARAN

Berdasarkan hasil penelitian ini, beberapa saran dapat diajukan untuk pengembangan lebih lanjut dari sistem pakar berbasis web yang menggunakan metode forward chaining untuk deteksi cybercrime:

6.1. Integrasi Pembelajaran Mesin

Penerapan pembelajaran mesin, seperti pembelajaran yang diawasi, dapat membantu sistem pakar mengenali pola ancaman baru yang tidak ada dalam basis pengetahuan, sehingga meningkatkan kemampuan adaptasinya terhadap serangan yang lebih kompleks.

6.2. Optimisasi Sekala Besar

Pengujian lebih lanjut di lingkungan dengan lalu lintas data tinggi, seperti jaringan perusahaan besar, diperlukan untuk memastikan kinerja optimal. Penerapan teknik penyeimbangan beban dan pemrosesan paralel dapat membantu meningkatkan efisiensi deteksi.

6.3. Pengembangan Notifikasi dan Antarmuka Pengguna

Peningkatan antarmuka pengguna dan sistem notifikasi yang lebih responsif membantu administrator dengan cepat memahami dan mengatasi ancaman. Fitur dasbor interaktif yang menampilkan aktivitas jaringan secara real-time juga meningkatkan manajemen ancaman.

DAFTAR PUSTAKA

[1] G. Brown, "The Customary International Law of Cyberspace," *Strategic Studies,* vol. 6, no. 3, pp. 126-145, 2012.

[2] Karunia, "Protecting the digitized society—the challenge of balancing surveillance and privacy," vol. 4, 2016.

[3] N. Choucri, "Lost in cyberspace: Harnessing the Internet, international relations, and global security," *Bulletin of the Atomic Scientists,* vol. 68, no. 2, pp. 70-77, 2012.

[4] S. Das, "Impact of Cyber Crime: Issues and Challenges," *International Journal of Engineering Sciences & Emerging Technologies,* vol. 6, no. 2, pp. 142-153, 2013.

[5] M. McGuire, "Cyber crime: A review of the evidence," *Home Office Research Report 75,* pp. 1-35, 2013.

[6] J. Iqbal, "Cybercrime in India : Trends and Challenges," *International Journal of Innovations & Advancement in Computer Science,* vol. 6, no. 12, pp. 187-196, 2017.

[7] J. Malik, "A Brief Review on Cyber Crime-Growth and Evolution," *Pramana Research Journal,* vol. 9, no. 3, pp. 242-278, 2019.

[8] A. C. Onuora, "The Challenges of Cybercrime in Nigeria: An Overview," *AIPFU Journal of School of Sciences (AJSS),* vol. 1, no. 2, pp. 6-11, 2017.

[9] M. A. D. Putri, "Sistem Pakar Mendeteksi Tindak Pidana Cybercrime Menggunakan Metode Forward Chaining Berbasis Web Di Kota Batam," *Edik Informatika,* vol. 3, no. 2, pp. 197-210, 2017.

[10] D. A. Arifah, "KASUS CYBERCRIME DI INDONESIA Indonesia's Cybercrime Case," *Jurnal Bisnis dan Ekonomi (JBE),* vol. 18, no. 2, pp. 185 - 195, 2011.