JISKa, Vol. 4, No. 3, JANUARI, 2020, Pp. 27 – 35
ISSN : 2527 – 5836 (print) | 2528 – 0074 (online)

DESAIN DAN IMPLEMENTASI SIMULASI *INTRUSION INDEX* BERBASIS SISTEM PAKAR DENGAN METODE *FORWARD CHAINING*

Mardian [(1)], H. Jemakmun [(2)], Linda Atika [(3)]
Program Pascasarjana Universitas Bina Darma
Jl. Jenderal Ahmad Yani No.3, 9/10 Ulu, Kecamatan Seberang Ulu I, Kota Palembang, Sumatera Selatan 30111
e-mail : mardiannelwan@gmail.com [(1)], jemakmun@binadarma.ac.id [(2)], linda.atika@binadarma.ac.id [(3)]

Abstract

Today's internet needs are increasing, the interest and attention on the internet is also getting wider and faster on the internet network, especially from disruption of attacks or illegal access to the internet network itself. Network ssecurity depends on the speed of nework setting in the case or following up the system when an interruption occurs. For this reason, software is needed that is capable of detecting and measurement attacks using an expert system. The results of the design and simulation carried out in this study can illustrate the way or flow of the use of the system from the manager who becomes an actor, to shows how the flow of information flows in a system and can provide a static picture of the system that shows relationships or interconnected relationships between classes related to information systems expert system for internet network security and the application of intrusion index to dassify the types of attacks into three levels, namely Deflect, Prevent, and Preempt by applying inference engine into Forward Chaining method.

Keywords**: **expert systems, network security, forward chaining method

Abstrak

Adanya kebutuhan internet yang semakin meningkat, ketertarikan dan perhatian pada internet juga semakin luas dan cepat sehingga harus diseimbangi dengan keamanan yang lebih cepat pada jaringan internet, terutama dari hal gangguan serangan atau akses ilegal pada jaringan internet. Keamanan jaringan bergantung pada kecepatan pengaturan jaringan dalam hal menindaklanjuti sistem saat terjadi gangguan. Untuk itu diperlukan suatu perangkat lunak yang mampu melakukan deteksi dan pengukuran serangan dengan menggunakan sistem pakar. Hasil dari desain dan simulasi yang dilakukan dalam penelitian ini dapat menggambarkan cara atau alur penggunaan sistem dari pengelola yang menjadi aktor, memperlihatkan cara aliran informasi mengalir dalam suatu sistem serta dapat memberikan gambaran sistem secara statis yang memperlihatkan relasi atau hubungan antarkelas yang saling berkaitan mengenai sistem informasi sistem pakar untuk keamanan jaringan internet dan penerapan *intrusion index* yang dapat menggolongkan jenis serangan ke dalam tiga tingkatan yaitu *deflect*, *prevent*, dan *preempt* dengan menerapkan mesin inferensi ke dalam metode *forward chaining*.

Kata Kunci : sistem pakar, keamanan jaringan, metode *forward chaining, Intrusion Index*

1. PENDAHULUAN

Adanya kebutuhan internet yang semakin meningkat, ketertarikan dan perhatian pada internet juga semakin luas dan cepat sehingga harus diseimbangi dengan keamanan yang lebih cepat pada jaringan internet, terutama dari hal gangguan serangan atau akses ilegal pada jaringan internet. Keamanan jaringan bergantung pada kecepatan pengatur jaringan dalam hal menindaklanjuti sistem saat terjadi gangguan. Pada penelitian sebelumnya menurut (Sodiya, Adeniran, & Ikuomola, 2007) , Ada 3 (tiga) jenis golongan atau rule yaitu 1. *Deflect* Jika terdapat serangan di dalam database 2. *Prevent* Jika terdapat gangguan di jaringan. 3. *Preempt* Jika terdapat gangguan yang lebih parah, baik di database maupun di jaringan yang sifatnya

berlanjut. *Intrusion Index* adalah suatu proses yang digunakan untuk mengukur dan mengetahui bahaya serangan yang dilakukan oleh seseorang ketika gangguan terdektesi.

Untuk menganalisa hal tersebut maka diperlukan sebuah pengukuran jenis golongan serangan yang terjadi dan analisa struktur basis data sistem pakar agar mudah digunakan oleh seorang administrator secara efektif sehingga penelitian bisa mengetahui sistem yang mampu memberikan respon secara cepat terhadap sistem pemberi peringatan seperti IDS sehingga seorang administrator dapat mengetahui apa pengertian arti peringatan tersebut dan bagaimana mengefektifkan respon tersebut. sehingga penelitian bisa mengetahui keefektifan metode *forward chaining* dalam memproses *Intrusion Index*.

Sistem pakar akan menjadi layaknya seorang pakar didalam bidang tertentu sesuai kebutuhan manusia. Sistem pakar mampu memecahkan masalah yang biasanya hanya dapat dipecahkan oleh seorang pakar dengan menggunakan pengetahuan, fakta dan teknik penalaran (Desiani, 2006)

Salah satu cara representasi *knowledge* (pengetahuan) adalah melalui *rule*. *Rule* merupakan struktur *IF/THEN* yang secara logika menghubungkan informasi yang tersimpan dalam bagian *IF* yang juga dikenal sebagai premis, dengan informasi yang tersimpan dalam bagian *THEN*. Kumpulan *rule* yang saling terkait disebut juga sebagai *rule set*. Bentuk umum *rule* sebagai berikut (Turban, 1995)

1. METODOLOGI PENELITIAN

Langkah pertama dalam penelitian ini adalah pengumpulan data dan analisis kebutuhan. Sumber pengumpulan data adalah penelitilan sebelumnya dan literature yang bersumber dari internet. Langkah kedua adalah mendesain struktur basis data. Langkah ketiga adalah pengukuran *Intrusion Index* dimana digunakan untuk mengukur dan mengetahui bahaya serangan yang dilakukan oleh seseorang ketika gangguan terdeteksi. Langkah keempat adalah pemrograman menggunakan visual studio. Metode yang digunakan dalam penelitian ini adalah *forward chaining*.

1. Analisis Data

Tahap awal ini dilakukan analisa kebutuhan, analisa permasalahan yang muncul, analisa *user*. Metode yang biasa digunakan pada tahap ini adalah membaca manual dokumentasi, pada analisis awal ini juga dilakukan dengan mencari informasi yang pernah dibuat sebelumnya.
Metode data yang dipakai pada penelitian ini adalah deskritif kualitatif. Sedangkan metode analisis berorientasi objek yang digunakan pada penelitian ini adalah metode *Unified* (Hariyanto, 2004). Adapun tahapan analisis yang digunakan adalah :

a. Berpedoman pada kebutuhan pemakai sistem
b. Mengidentifikasi skenario pemakaian atau *usecase*
c. Memilih kelas-kelas dan objek menggunakan kebutuhan penuntun.
d. Mengidentifikasi atribut dan operasi masing-masing kelas objek
e. Mengidentifikasi struktur dan hirarki kelas-kelas.
f. Membangun model keterhubungan kelas dan objek

2. Desain

Desain antarmuka dalam penelitian ini berupa halaman *login*, desain halaman berhasil *login*, desain menu utama dan desain jika terjadi serangan yang akan memberikan gambaran jelas tentang penelitian. Biasanya hasil dari desain berupa.

a. *Use case*, kelas diagram dan tampilan visual sistem pakar
b. Gambar-gambar detil estimasi kebutuhan yang ada

3. Implementasi

Dalam fase implementasi akan diterapkan semua yang telah direncanakan dan pembuatan modul yang telah dirancang sebelumnya sesuai dengan bahasa pemograman yang digunakan dalam sistem yang akan dibangun. Implementasi sistem akan dilakukan dengan spesifikasi berikut:

a. Sistem operasi *Windows 7*
b. Memori 2 GB
c. Bahasa Pemrograman *C++*
d. *Compiler* Visual Studio

2. HASIL DAN PEMBAHASAN

Penelitian ini hanya didasarkan pada simulasi aplikasi yang bersifat *offline* tanpa dilakukan pengujian. Pengujian pengguna akan dilakukan di riset pengembangan selanjutnya ketika aplikasi benar-benar dijalankan dalam jaringan internet. Pada gambar 1 bisa dilihat dengan jelas bahwa sistem pakar memiliki *rule base*, *database* dan *inference engine*. Mesin inferensi yang dikembangkan dalam sistem pakar ini menggunakan aturan untuk menghasilkan hasil diagnosis berdasarkan data dan fakta penelitian sebelumnya dan melakukan pengukuran dengan *Intrusion Index* yang menggunakan perhitungan sebagai berikut (Sodiya et al., 2007).

R1 : *IF II is low THEN Deflect*
R2 : *IF II is high THEN Prevent*
R3 *: IF II is very high THEN Preempt*

$$\textit{Intrusion Index}\ (\mathrm{II}) = \frac{\sum_{i=1}^{n} X_i}{\sum_{i=1}^{n} X_{i\ \max()}}$$

Dimana: untuk *n* = 3 (karena ada tiga variabel)

Variabel untuk perhitungan tersebut adalah

a)	Kategori Serangan	Skor
	Confidentiality	1
	Integrity	2
	Availability	3
b)	Dampak Serangan	Skor
	Low	1
	High	2
	Very High	3
c)	Tingkat Pelanggaran Keamanan	
	Low	1
	High	2
	Very High	3

X = Variabel skor
$X_{i\ \max(\ )}$ = Skor maksimum yang diperoleh untuk variabel *i*
Nilai maksimum untuk *instrusion* adalah 1 (satu), yang mana dibagi menjadi tiga rating sebagai berikut:

1. *Intrusion Index* akan bernilai rendah ketika $0 \leq II < 0{,}3$
2. *Intrusion Index* akan bernilai tinggi ketika $0{,}3 \leq II < 0{,}7$
3. *Intrusion Index* akan bernilai sangat tinggi ketika $0{,}7 \leq II < 1$

Ini berarti bahwa jika indeks yang dihitung antara 0 dan 0,3, maka Intrusin Indek bernilai rendah, dan seterusnya.

Jika terjadi sebuah serangan dengan kategori *confidentiality* yang bernilai 1, *attack implication* bernilai 3, dan *security violation level* bernilai 2. maka perhitungan nya sebagai berikut:

$$\sum_{i=1}^{3} 1 + 3 + 2 = 6$$

dan untuk nilai $Xi_{max(\ )}$, nilai yang di dapat terdiri dari skor tertinggi yaitu *attack category* bernilai 3, *attack implication* bernilai 3, dan *security violation level* bernilai 3:

$$\sum_{i=1}^{3} 3 + 3 + 3 = 9$$

sehingga :

$$= \frac{\sum_{i=1}^{n} Xi}{\sum_{i=1}^{n} Xi \max()}$$

$$= \frac{\sum_{i=1}^{3} 1 + 3 + 2 = 6}{\sum_{i=1}^{3} 3 + 3 + 3 = 9}$$

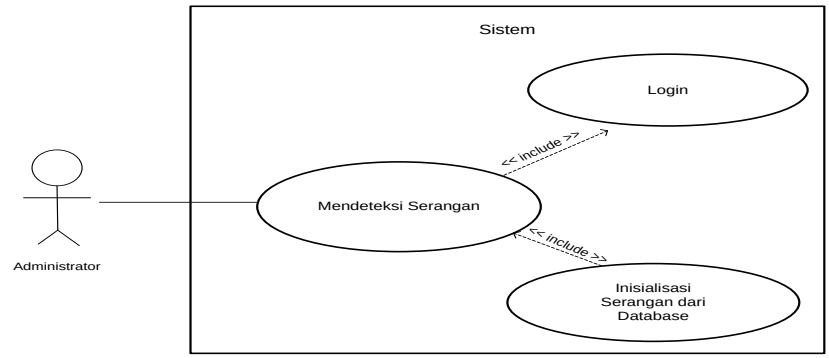
$$= \frac{6}{9} \text{ atau } \frac{2}{3}$$

$$= 0{,}6 \text{ (High)}$$

Dalam simulasi ini *rule base* di klasifikasikan menjadi tiga macam pesan yaitu:

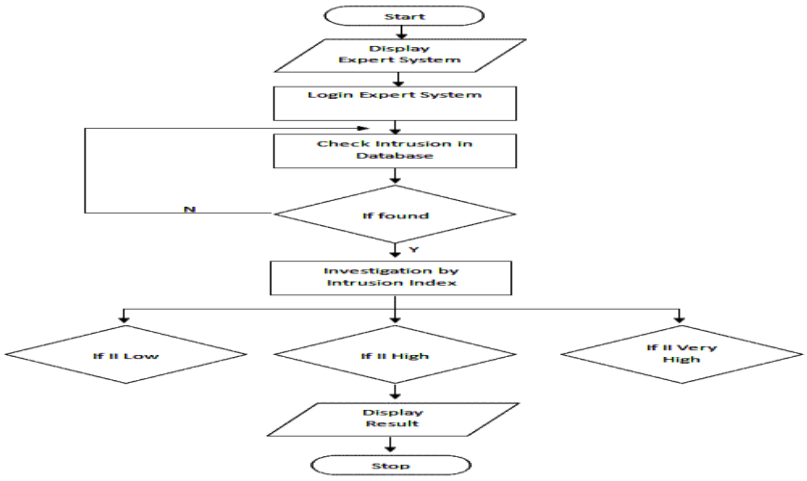
1. *Deflect* : Memberikan peringatan ke admin agar waspada terhadap serangan.
2. *Prevent*: Memberikan peringatan ke admin agar mencegah penyusup dari jaringan lokal.
3. *Preempt*: Memberikan peringatan ke admin agar memutuskan koneksi komputer atau PC yang telah diserang

Pada gambar 2 diagram *use case* bisa dilihat bahwa aktor utama pada sistem ini adalah seorang administrator yang sudah terverifikasi dan harus *login* terlebih dahulu sebelum menggunakan sistem. Administrator otomatis menuju halaman deteksi serangan untuk dapat melihat atau memonitoring kondisi jaringan. *Use case* diagram merupakan suatu model yang fungsinal dalam sistem yang menggunakan aktor dan use *case* (Aditiawarman, 2017).



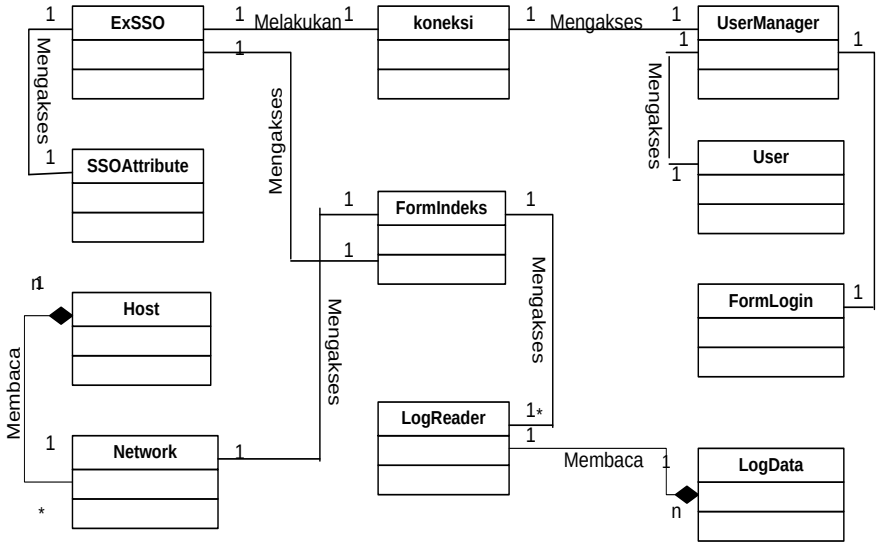
Gambar 1 Diagram *Use Case*

Gambar 1 menjelaskan bagaimana sistem pakar bekerja ketika seorang administrator telah berhasil login maka sistem akan melakukan pengecekan di database dan mengelola database tersebut dengan perhitungan *intrusion index* jika terjadi serangan apakah termasuk kategori *low, high* dan *very high* sehingga sistem pakar akan otomatis menampilkan hasil keputusan apa yang harus dilakukan oleh seorang administrator dalam menyikapi serangan yang terjadi.



Gambar 2 *Flow chart*

Pada gambar 4 terdapat 11 (sebelas) kelas yaitu *Exsso, SSOAttribute,Host, Network, Koneksi, FormIndeks, Logreader, user manager, user, Form Login* dan *Log Data*, dimana masing-masing kelas mempunyai *method* dan atribut.



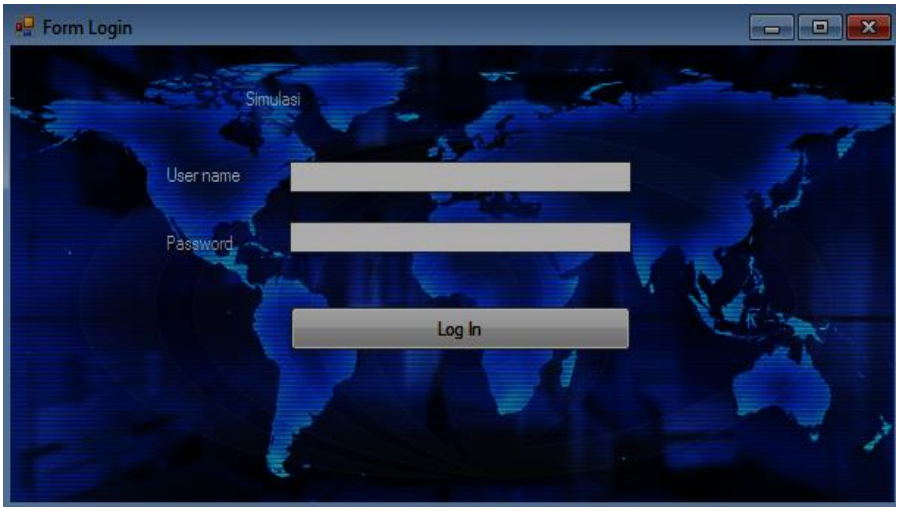
Gambar 3 Kelas Diagram Keseluruhan

Kelas ExSSO merupakan kelas kontrol yang menangani perhitungan sistem pakar pada sistem. Kelas *SSOAttribute* merupakan kelas entitas yang menangani data-data ke database. Kelas *Host* merupakan kelas entitas yang berfungsi menyediakan data-data informasi komputer penyerang. Kelas *Network* merupakan kelas kontrol yang menghubungkan kelas *Host* dan kelas antarmuka *FormIndeks*. Kelas koneksi merupakan kelas koneksi yang menghubungkan kelas ExSSO dan kelas *UserManager*. Kelas *FormIndeks* merupakan kelas antarmuka yang menangani tampilan menu utama dan berperan sebagai induk aplikasi. Kelas *LogReader* adalah kelas yang berfungsi membaca *filelog* untuk ditampilkan pada sistem. Kelas *UserManager* merupakan kelas *control* yang mengatur *username* dan *password* admin. Kelas *User* merupakan kelas entitas untuk *username* dan *password* admin. Kelas *FormLogin* merupakan kelas antarmuka yang menangani tampilan menu *Login* untuk mengakses sistem. Kelas *LogData* merupakan kelas yang mengatur data-data *log* seperti nama serangan,alamat IP,waktu,dan tanggal serangan.

Tabel 1 Seluruh Nilai *Intrusion Index* yang terpenuhi

No	*Security Violation Level*	*Attack Implication*	*Attack Category*	Hasil	Nilai *Intrusion Index*	Kategori Serangan
1.	1	1	1	3	0,3	Low
2.	1	1	2	4	0,4	High
3.	1	1	3	5	0,5	High
4.	1	2	1	4	0,4	High
5.	1	2	2	5	0,5	High
6.	1	2	3	6	0,6	High
7.	1	3	1	5	0,5	High
8.	1	3	2	6	0,6	High
9.	1	3	3	7	0,7	Very High
10.	2	1	1	4	0,4	High
11.	2	1	2	5	0,5	High
12.	2	1	3	6	0,6	High
13.	2	2	1	5	0,5	High
14.	2	2	2	6	0,6	High
15.	2	2	3	7	0,7	Very High
16.	2	3	1	6	0,6	High
17.	2	3	2	7	0,7	Very High
18.	2	3	3	8	0,8	Very High
19.	3	1	1	5	0,5	High
20.	3	1	2	6	0,6	High
21.	3	1	3	7	0,7	Very High
22.	3	2	1	6	0,6	High
23.	3	2	2	7	0,7	Very High
24.	3	2	3	8	0,8	Very High
25.	3	3	1	7	0,7	Very High
26.	3	3	2	8	0,8	Very High
27.	3	3	3	9	1	Very High

Rancangan antarmuka perangkat lunak yang dibangun. Sesuai analisa, ada beberapa kelas antarmuka (*interface*) yaitu *Form Login* dan *Form Indeks*. Adapun rancangan tampilan *Form* Utama sebagai berikut.



Gambar 4 Antarmuka *Form Login*

Pada gambar 8 Tampilan *form* apabila berhasil login dengan kecocokan *username* dan *password* yang diterima dan terdaftar di database. Saat tampilan berhasil login sudah ditampilkan maka form Indeks siap digunakan.

Gambar 5 Antarmuka berhasil *login*

Tampilan *form* apabila berhasil login dengan kecocokan *username* dan *password* yang diterima dan terdaftar di database. Saat tampilan berhasil login sudah ditampilkan maka form Indeks siap digunakan.

Gambar 6 Antarmuka *Form Indeks*

KESIMPULAN

Kesimpulan yang dapat ditarik berdasarkan hasil dari desain dan implementasi analisis basis data sistem pakar menggunakan metode *forward chaining* adalah berjalan dengan baik dan mengeluarkan hasil nilai sesuai yang diterapkan Sistem pakar adalah solusi yang nantiny akan membantu seorang administrator jaringan internet tentang keputusan apa yang diambil ketika terjadi serangan pada jaringan. Perhitungan *Intrusion index* sangat membantu dalam penentuan nilai yang berguna sebagai mesin inferensi sistem pakar. Sistem pakar ini diharapkan membantu akuisisi pengetahuan dari pakar ke sistem dan tidak menutup kemungkinan adanya pembaruan akuisisi pengetahuan dari pakar. Selain itu, memperbarui aturan juga menjamin yang baru pengetahuan dari para ahli karena tidak harus merusak aturan

dasar sistem. Tampilan antarmuka yang berkonsep visual grafis dapat memudahkan seorang administrator membaca informasi yang dikeluarkan oleh sistem pakar.

Keterbatasan penelitian adalah sistemnya masih dirancang hanya diterapkan sebagai simulasi dan sistem pakar ini belum diterapkan secara *online*. Karena itu, disarankan untuk penelitian masa depan atau selanjutnya untuk mengembangkan sistem pakar ini dengan bersifat *real time.*

DAFTAR PUSTAKA

Aditiawarman. (2017). *Sistem Pakar Pendeteksi Penyakit Mata Berbasis Android*. *5*(2).

Desiani, A. (2006). *Konsep Kecerdasan Buatan*. Yogyakarta: Andi Offset.

Hariyanto, B. (2004). *Sistem Manajemen Basis Data*. Bandug: Informatika.

Sodiya, A. S., Adeniran, O., & Ikuomola, R. (2007). An Expert System-based Site Security

Officer. *Journal of Computing and Information Technology*, *15*(3), 227–235.

https://doi.org/10.2498/cit.1000961

Turban, efraim. (1995). *Decision support and expert systems : management support systems*.