

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



TESIS

Oleh

MARDIAN

162420006

ENTERPRISE IT INFRASTRUCTURE

**PROGRAM STUDI TEKNIK INFORMATIKA - S2
PROGRAM PASCA SARJANA
UNIVERSITAS BINA DARMA
PALEMBANG
2019**

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

Tesis ini diajukan sebagai salah satu syarat
untuk memperoleh gelar

MAGISTER KOMPUTER



Oleh
MARDIAN
162420006
ENTERPRISE IT INFRASTRUCTURE

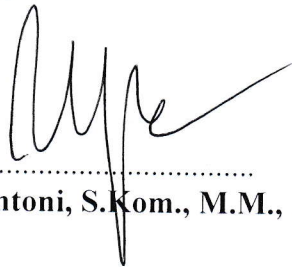
**PROGRAM STUDI TEKNIK INFORMATIKA - S2
PROGRAM PASCA SARJANA
UNIVERSITAS BINA DARMA
PALEMBANG
2019**

Halaman Pengesahan Pembimbing Tesis

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

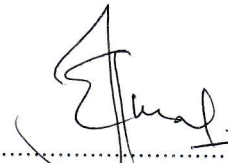
Oleh MARDIAN NIM 162420006 Tesis ini telah disetujui dan disahkan oleh Tim
Penguji Program Studi Teknik Informatika - S2 Konsentrasi ENTERPRISE IT
INFRASTRUCTURE Program Pascasarjana Universitas Bina Darma pada 07
September 2019 dan telah dinyatakan LULUS.

Palembang, 07 September 2019
Mengetahui,
Ketua Program studi



.....
Darius Antoni, S.Kom., M.M., Ph.D

Tim Pembimbing
Pembimbing I,



.....
Dr. H. Jemakmun, M.Si

Pembimbing II,



.....
Linda Atika, M.Kom

Halaman Pengesahan Penguji Tesis

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

Oleh MARDIAN NIM 162420006 Tesis ini telah disetujui dan disahkan oleh Tim
Penguji Program Studi Teknik Informatika - S2 konsentrasi ENTERPRISE IT
INFRASTRUCTURE, Program Pascasarjana Universitas Bina Darma pada 07
September 2019 dan telah dinyatakan LULUS.

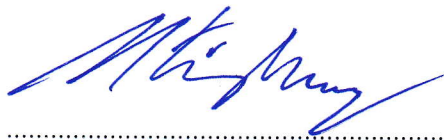
Palembang, 07 September 2019

Mengetahui,

Program Pascasarjana

Universitas Bina Darma

Direktur,



.....
Dr. Ir. Hj. Hasmawaty AR, M.M., M.T.

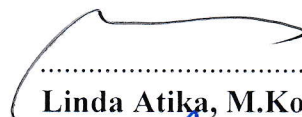
Tim Penguji :

Penguji I,



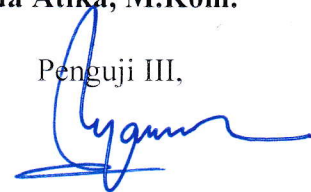
.....
Dr. H. Jemakmun, M.Si.

Penguji II,



.....
Linda Atika, M.Kom.

Penguji III,



.....
Dedy Syamsuar, Ph.D.

Penguji IV,



.....
Afriyudi, M.Kom

SURAT PERNYATAAN

Saya yang bertanda tangan dibawah ini:

Nama : MARDIAN

NIM : 162420006

Dengan ini menyatakan bahwa:

1. Karya tulis Saya (Tesis) ini adalah asli dan belum pernah diajukan untuk mendapatkan gelar akademik baik (Magister, Sarjana, dan Ahli Madya) di Universitas Bina Darma;
2. Karya tulis ini murni gagasan, rumusan dan penelitian Saya sendiri dengan arahan tim pembimbing;
3. Dalam karya tulis ini tidak terdapat karya atau pendapat yang telah ditulis atau dipublikasikan orang lain, kecuali secara tertulis dengan jelas dikutip dengan mencantumkan nama pengarang dan memasukkan ke dalam daftar pustaka;
4. Karena yakin dengan keaslian karya tulis ini, Saya menyatakan bersedia Tesis/Skripsi/Tugas Akhir, yang Saya hasilkan di unggah ke internet;
5. Surat Pernyataan ini Saya tulis dengan sungguh-sungguh dan apabila terdapat penyimpangan atau ketidakbenaran dalam pernyataan ini, maka Saya bersedia menerima sanksi dengan aturan yang berlaku di perguruan tinggi ini;

Demikian Surat Pernyataan ini saya buat agar dapat dipergunakan sebagaimana mestinya.

Palembang, 07 September 2019

Yang Membuat Pernyataan,



MARDIAN

NIM: 162420006

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. 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*

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 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

MOTTO DAN PERSEMBAHAN

Seputih kapas sebening embun pagi,

Dikala sang surya menerangi bumi untuk kehidupan mahluknya,

Dan kala malam telah menyelimuti seluruh jagad.

Terimakasih Bapak, Ibu yang melahirkan ku

Terimakasih Bapak, Ibu yang telah membesarkan dan membekali ilmu

Dan Terimakasih Bapak, Ibu yang saat ini membimbing anak-anak ku

Aku hanya dapat mempersembahkan tulisan ini kepadamu, sebagai

Baktiku.

Juga untuk istriku tercinta Fitriana

dan anak ku Lashira Mardian

“Dan Tiadalah kehidupan dunia ini, selain dari main-main dan senda gurau belaka. Dan sungguh kampung akhirat itu lebih baik bagi orang-orang yang bertaqwa. Maka tidakkah kamu memahaminya?” (QS. Al-An’am: 32)

KATA PENGANTAR



Alhamdulillah, atas segala nikmat yang diberikan oleh Allah SWT yang selalu memberikan berkah, rahmat dan karunia-Nya sehingga penulis dapat menyelesaikan tesis yang berjudul Desain dan Implementasi Simulasi Intrusion Index berbasis Sistem Pakar dengan Metode *Forward Chaining*.

Tesis ini disusun sebagai salah satu syarat untuk memperoleh gelar Magister Komputer pada Universitas Bina Darma Palembang. Dalam penulisan tesis ini penulis telah berusaha semaksimal mungkin memberikan dan menyajikan yang terbaik. Tetapi penulis juga menyadari bahwa penelitian ini masih jauh dari sempurna, hal ini dikarenakan terbatasnya pengetahuan yang dimiliki penulis. Oleh karena itu, penulis mengharapkan saran dan kritik yang bersifat membangun untuk kesempurnaan tesis ini.

Pada kesempatan ini, tidak lupa penulis mengucapkan terimah kasih kepada semua pihak yang telah memberikan bimbingan, pengarahan, nasihat, dan pemikiran dalam menyelesaikan tesis ini, terutama kepada :

1. Dr. Sunda Ariana, M.Pd., M.M. selaku Rektor Universitas Bina Darma Palembang
2. Dr. Ir. Hasmawaty AR, M.M., M.T. selaku Direktur Pascasarjana Universitas Bina Darma Palembang
3. Dedy Syamsuar, Ph.D. Selaku Dekan Fakultas Ilmu Komputer Universitas Bina Darma Palembang.
4. Darius Antoni, S.Kom., M.M., Ph.D. Selaku Ketua Program Studi Magister Informatika Universitas Bina Darma Palembang.
5. Dr. H. Jemakmun, M.Si. Selaku Pembimbing I yang telah memberikan bimbingan tesis ini.
6. Linda Atika, M.Kom. Selaku pembimbing II yang telah memberikan bimbingan dan arahan dalam penulisan tesis ini.

7. Pihak Sekretariat Pascasarjana Universitas Bina Darma Palembang yang telah memberikan bimbingan pelayanan dengan baik.

Palembang, 06 September 2019

Penulis

Mardian

162420006

DAFTAR ISI

	<i>Halaman</i>
HALAMAN JUDUL	i
HALAMAN PENGESAHAN PEMBIMBING TESIS	ii
HALAMAN PENGESAHAN PENGUJI TESIS	iii
SURAT PERNYATAAN	iv
ABSTRAK	v
ABSTRACT	vi
MOTTO DAN HALAMAN PERSEMBAHAN	vii
KATA PENGANTAR.....	viii
DAFTAR ISI.....	ix
DAFTAR TABEL	x
DAFTAR GAMBAR.....	xi
DAFTAR LAMPIRAN	xii
BAB I. PENDAHULUAN	
1.1 Latar Belakang	1
1.2 Identifikasi Masalah	2
1.3 Batasan Masalah	2
1.4 Rumusan Masalah	3
1.5 Tujuan Penelitian	3
1.6 Manfaat Penelitian	3
1.7 Ruang Lingkup.....	4
1.8 Susunan dan Struktur Tesis.....	4
BAB II. KAJIAN PUSTAKA	
2.1 Pengertian Keamanan Jaringan	5
2.1.1 Jenis <i>Intrusion Detection System</i>	8
2.1.2 Kebutuhan <i>Intrusion Detection System</i>	9
2.2 Pengertian <i>Filelog</i>	10
2.3 Jaringan Komputer	11
2.4 Internet Protokol	11

2.4.1 (<i>File Transfer Protocol</i>) FTP	12
2.4.2 <i>Hyper T ext Transfer Protocol</i> (HTTP)	12
2.4.3 <i>Address Resolution Protocol</i> (ARP)	12
2.4.4 <i>Internet Control Message Protocol</i> (ICMP).....	13
2.4.5 <i>User Datagram Protocol</i> (UDP).....	13
2.5 Pengertian Sistem Pakar	13
2.5.1 Komponen Sistem Pakar	18
2.5.2 <i>Inference Engine</i>	21
2.5.3 Metode <i>Forward Chaining</i>).....	22
2.5.4 <i>Intrusion Index</i>	23
2.5.5 <i>Interpreter</i>	26
2.5.6 <i>Rule Base</i>	27
2.5.7 Kerangka Pemikiran	28

BAB III. METODOLOGI PENELITIAN

3.1 Metode Penelitian yang Digunakan	29
3.2 Teknik Pengumpulan Data	30
3.2.1 Jenis Data	30
3.2.2 Sumber Data	30
3.2.3 Metode Pengumpulan Data	30
3.3 Metode Analisis Data	31
3.4 Metode Analisis Pengembangan	31
3.4.1 Analisis	31
3.4.2 Desain	31
3.4.3 Implementasi	32
3.4.4 Simulasi	32
3.4.5 Monitoring	32

BAB IV. ANALISA DAN PEMBAHASAN

4.1 Analisis <i>Rule</i> Sistem Pakar	33
4.1.1 Analisis Inferensi (<i>Inference Engine</i>)	34
4.1.2 <i>Intrusion Index</i>	35
4.2 Analisis Perangkat Lunak	37

4.2.1 Deskripsi Umum Perangkat Lunak	37
4.2.2 Analisis Kebutuhan Perangkat Lunak	37
4.3 Model Use Case	38
4.3.1 Diagram Use Case	38
4.3.2 Definisi Aktor	39
4.3.3 Definisi Use Case	39
4.3.4 Skenario Use Case	40
4.3.4.1 Skenario Use Case Login	40
4.3.4.2 Skenario Use Case Mendeteksi Serangan	41
4.3.4.3 Kelas Analisis	43
4.3.4.4 Sequence Diagram	44
4.3.4.5 Kelas Diagram	46
4.3.4.5.1 Kelas Diagram Keseluruhan	46
4.3.4.5.2 Rincian Kelas Diagram Tiap Use Case	47
4.4 Uji Perangkat Lunak	52
4.4.1 Data	52
4.4.2 Analisis Antarmuka	53
4.4.3 Lingkungan Uji Analisa	55
4.4.4 Uji Kelas	56
4.4.5 Antarmuka	59
4.5 Penguji Perangkat Lunak	60
4.5.1 Rencana Pengujian	61
4.5.2 Kasus Uji	62
4.5.3 Hasil Analisa Pengujian <i>Inference Engine</i>	65

BAB V. KESIMPULAN DAN SARAN

5.1 Kesimpulan	73
5.2 Saran	74

DAFTAR PUSTAKA

DAFTAR RIWAYAT HIDUP

LAMPIRAN

DAFTAR TABEL

	<i>Halaman</i>
Tabel 4.1. Kategori Serangan	35
Tabel 4.2. Dampak Serangan	35
Tabel 4.3. Tingkat Pelanggaran Keamanan	36
Tabel 4.4 Serangan Berdasarkan Kategori.....	38
Tabel 4.5 Serangan Berdasarkan Nilai Kategori.....	38
Tabel 4.6. Kebutuhan Fungsional	40
Tabel 4.7. Kebutuhan Non Fungsional	40
Tabel 4.8. Definisi Aktor	41
Tabel 4.9. Definisi <i>Use case</i>	42
Tabel 4.10. Skenario <i>Use case Login</i>	42
Tabel 4.11. Skenario <i>Use case</i> Mendeteksi Serangan.....	44
Tabel 4.12. Kelas Diagram <i>FormLogin</i>	49
Tabel 4.13. Kelas Diagram <i>Form Indeks</i>	49
Tabel 4.14. Kelas Diagram <i>ExSSo</i>	50
Tabel 4.15. Kelas Diagram <i>SSOAttribute</i>	51
Tabel 4.16. Kelas Diagram <i>Host</i>	51
Tabel 4.17. Kelas Diagram Koneksi.....	52
Tabel 4.18. Kelas Diagram <i>LogData</i>	52
Tabel 4.19. Kelas Diagram <i>LogReader</i>	53
Tabel 4.20. Kelas Diagram <i>Network</i>	53
Tabel 4.21. Kelas Diagram <i>User</i>	53
Tabel 4.22. Kelas Diagram <i>User Manager</i>	54
Tabel 4.23. Tabel <i>Administrator</i>	54
Tabel 4.24. Tabel <i>PC</i>	55
Tabel 4.25. Tabel <i>Attack Category</i>	55
Tabel 4.26. Daftar Implementasi Kelas.....	58
Tabel 4.27. Rencana Pengujian <i>Use case Login</i>	63
Tabel 4.28. Rencana Pengujian <i>Use case</i> Mendeteksi Serangan	63

Tabel 4.29.	Kasus Uji <i>Use case Login</i>	64
Tabel 4.30.	Kasus Uji <i>Use case Mendeteksi Serangan</i>	65
Tabel 4.31.	Hasil Tingkat Serangan	70

DAFTAR GAMBAR

	Halaman
Gambar 2.1. Jenis-jenis IDS dan Contoh Serangan yang di Deteksi	9
Gambar 2.2. Arsitektur Rancangan IDS Berbasis Sistem Pakar.....	27
Gambar 4.1. Diagram <i>Use case</i>	38
Gambar 4.2. Kelas Analisis <i>Login</i>	43
Gambar 4.3. Kelas Analisis Mendeteksi Serangan	43
Gambar 4.4. <i>Sequence Diagram Use case Login</i>	44
Gambar 4.5. <i>Sequence Diagram Use case</i> Mendeteksi Serangan.....	45
Gambar 4.6. Kelas Diagram Keseluruhan	46
Gambar 4.7. Tampilan Antarmuka <i>Form Login</i>	53
Gambar 4.8. Tampilan Antarmuka Berhasil <i>Login</i>	54
Gambar 4.9. Tampilan Antarmuka <i>Form Indeks</i>	55
Gambar 4.10. Tampilan Antarmuka <i>Form Login</i>	59
Gambar 4.11. Antarmuka <i>Form Indeks</i>	60
Gambar 4.12. <i>Intrusion Index</i>	65
Gambar 4.13. Penilaian <i>Intrusion Index</i>	66
Gambar 4.14. <i>Intrusion Index</i> Mengukur Bahaya Serangan.....	67
Gambar 4.15. Deteksi Serangan Dengan Tingkat Rendah <i>Low</i>	69
Gambar 4.16. Deteksi Serangan Dengan Tingkat Tinggi <i>High</i>	70
Gambar 4.17. Deteksi Serangan Dengan Tingkat Sangat Tinggi <i>Very High</i>	70

DAFTAR LAMPIRAN

Lampiran 1	SK Pembimbing
Lampiran 2	Lembar Konsultasi Tesis
Lampiran 3	Jurnal
Lampiran 4	Sertifikat Kunjungan Industri
Lampiran 5	Sertifikat Seminar Nasional
Lampiran 6	Riwayat Hidup