# ANALISA SISTEM KEAMANAN *INTRUSION DETECTION SYSTEM* (IDS), *FIREWALL SYSTEM, DATABASE SYSTEM* DAN *MONITORING SYSTEM* MENGGUNAKAN AGENT BERGERAK

**Bambang Sugiantoro[1)], Jazi Eko Istianto[2)]**
[1,2)] Program Pasca Sarjana Ilmu Komputer Fakultas Matematika dan Ilmu Pengetahuan Alam Universitas Gadjah Mada Yogyakarta
Jl Sekip Utara Bulaksumur Yogyakarta 55281
e-mail : bambang05@gmail.com , jazi@ugm.ac.id

**Abstrak**
*Keamanan jaringan komputer sebagai bagian dari sebuah sistem informasi adalah sangat penting untuk menjaga validitas dan integritas data serta menjamin ketersediaan layanan bagi penggunanya. Sistem harus dilindungi dari segala macam serangan dan usaha-usaha penyusupan atau pemindaian oleh pihak yang tidak berhak.Metode kemanan jaringan yang bertujuan untuk membentuk suatu arsitektur sistem keamanan yang terintegrasi antara Intrusion Detection System (IDS) , Firewall System, Database System dan Monitoring System dikaitkan dengan tinjauan agent bergerak. Sistem keamanan ini bertujuan melindungi jaringan dengan kemampuan merespon sesuai dengan kebijakan keamanan. Dihasilkan Arsitektur suatu sistem deteksi penyusupan jaringan komputer yang memiliki kemampuan untuk mendeteksi adanya aktivitas jaringan yang mencurigakan, melakukan tindakan penanggulangan serangan lebih lanjut berbasis agent bergerak*
***Keyword** : Intrusion Detection System ,Agent bergerak , Keamanan Jaringan Komputer*

## 1. PENDAHULUAN

Jaringan komputer terus mengalami perkembangan, baik dari skalabilitas, jumlah node dan teknologi yang digunakan. Hal ini memerlukan pengelolaan jaringan yang baik agar ketersediaan jaringan selalu tinggi. Tugas pengelolaan jaringan yang dilakukan administrator jaringan memiliki banyak permasalahan, diantaranya yang berkaitan dengan keamanan jaringan komputer. Penyusupan (intrusion) adalah seseorang yang berusaha merusak atau menyalahgunakan sistem, atau setiap usaha yang melakukan compromise integritas,kepercayaan atau ketersediaan suatu sumberdaya komputer . Definisi ini tidak bergantung pada sukses atau gagalnya aksi tersebut, sehingga berkaitan dengan suatu serangan pada sistem komputer. Intrusion detection (ID) singkatnya adalah usaha mengidentifikasi adanya penyusup yang memasuki sistem tanpa otorisasi (misal cracker) atau seorang user yang sah tetapi menyalahgunakan (abuse) privelege sumberdaya sistem ( misal insider threath) . Intrusion Detection System (IDS) atau Sistem Deteksi Penyusupan adalah sistem komputer (bisa merupakan kombinasi software dan hardware) yang berusaha melakukan deteksi penyusupan . IDS akan melakukan pemberitahuan saat mendeteksi sesuatu yang dianggap sebagai mencurigakan atau tindakan ilegal. IDS tidak melakukan pencegahan terjadinya penyusupan. Pengamatan untuk melakukan pemberitahuan itu bergantung pada bagaimana baik melakukan konfigurasi IDS. Software Agent (selanjutnya disebut agent saja) adalah entitas perangkat lunak yang didedikasikan untuk tujuan tertentu . Agen bisa memiliki ide sendiri mengenai bagaimana menyelesaikan suatu pekerjaan tertentu. Sejumlah riset tentang agentelah membuat bermacam aplikasi, misal untuk distributed meeting scheduler, network mapping,auction, dan searching database.Masalah keamanan dan kerahasiaan merupakan salah satu aspek penting dari suatu pesan, data, atau informasi. Dalam hal ini sangat terkait dengan betapa pentingnya pesan, data, atau informasi tersebut di kirim dan di terima oleh pihak atau orang yang berkepentingan, apakah pesan, data, atau informasi masih *authenticity*. Pesan, data, atau informasi akan tidak berguna lagi apabila di tengah jalan informasi itu disadap atau dibajak oleh orang yang tidak berhak atau berkepentingan.( firrar.U., Riyanto B , 2003 )

## 2. TINJAUAN PUSTAKA

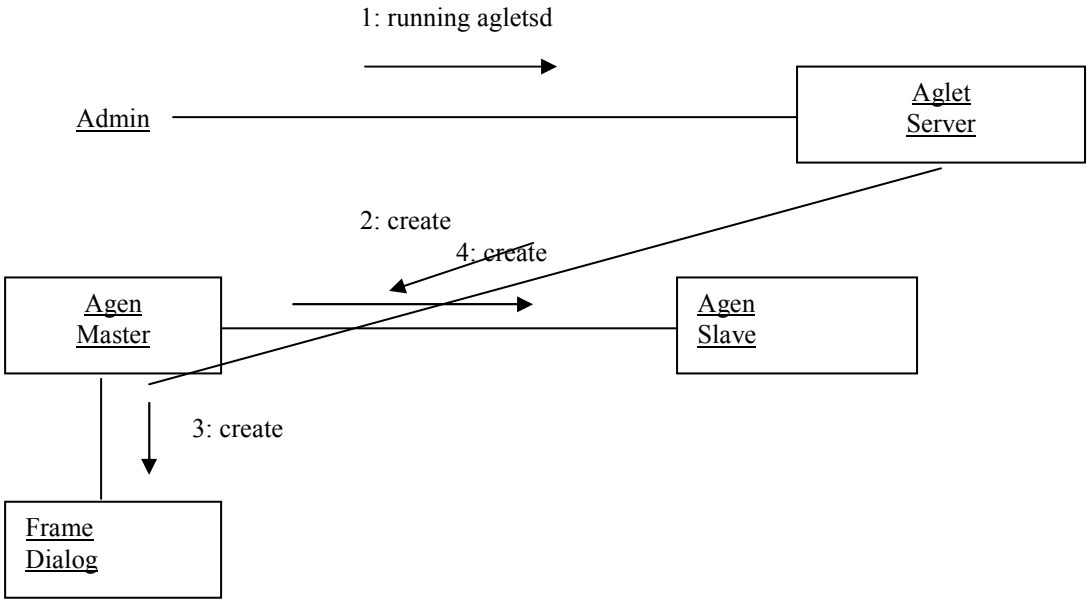
Pada penelitian sebelumnya telah dilakukan desain dan implementasikan suatu sistem deteksi penyusupan jaringan yang memiliki kemampuan untuk mendeteksi adanya aktivitas jaringan yang mencurigakan, melakukan tindakan penanggulangan serangan lebih lanjut, serta mampu berinteraksi dengan administrator menggunakan media SMS (Short Message Service) dua arah( Gunawan Adi S, 2003 ). Pada paper ini akan dikaji sistem sensor diganti menggunakan framework agent bergerak.

## 3. METODE PENELITIAN

Metode penelitian dilakukan : pengumpulan data dari berbagai literatur tentang sistem keamanan dan agent bergerak , tahap kedua dibuat perancangan arsitektur sistem , perancangan IDS , perancancangan agent bergerak , perancangan database server , perancangan monitoring sistem dan perancangan notifikasi sistem. Belum dilakukan tahap implementasi dan pengujian sistem.

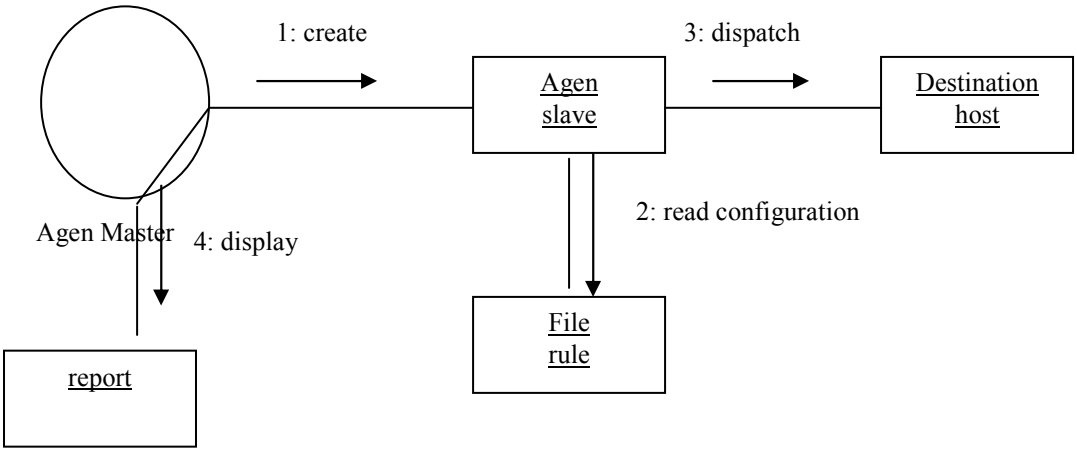
## 4. HASIL DAN PEMBAHASAN

Arsitektur sistem keamanan yang terintegrasi antara Intrusion Detection System (IDS) , Firewall System, Database System dan Monitoring System menggunakan pendekatan agent bergerak . Sistem keamanan ini bertujuan melindungi jaringan dengan kemampuan merespon sesuai dengan kebijakan keamanan.



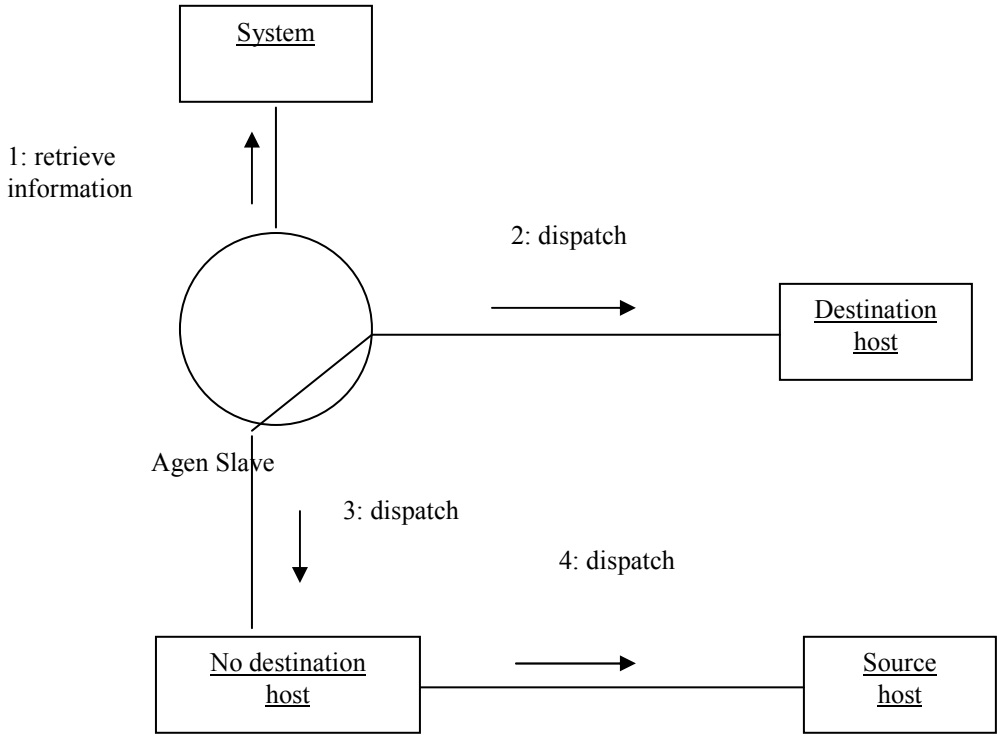

**Gambar 1.** Collaboration diagram agent

Selanjutnya agen Slave membaca file konfigurasi yang diperlukan untuk menentukan pengambilan informasi dan kebijakan jaringan. Lalu dispatch agen Slave lewat jaringan ke host tujuan. Langkahnya dapat dilihat pada diagram kolaborasi di gambar dibawah



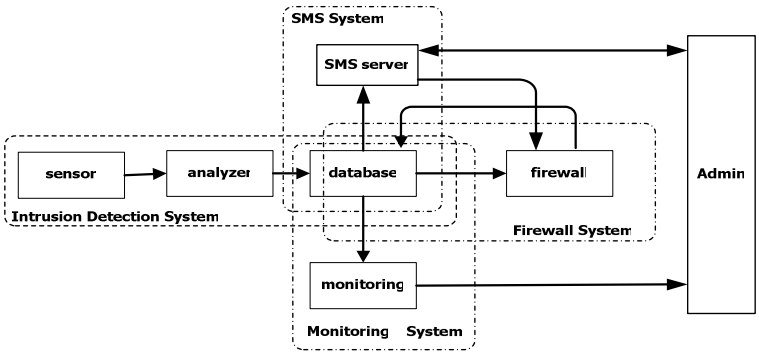

**Gambar 2** Collaboration diagram dispatching agent

Sesampai di host tujuan, agen Slave akan mengumpulkan informasi deteksi penyusupan yang diperlukan. Bila tidak ada lagi host tujuan maka agen Slave akan kembali ke host asal pengiriman.



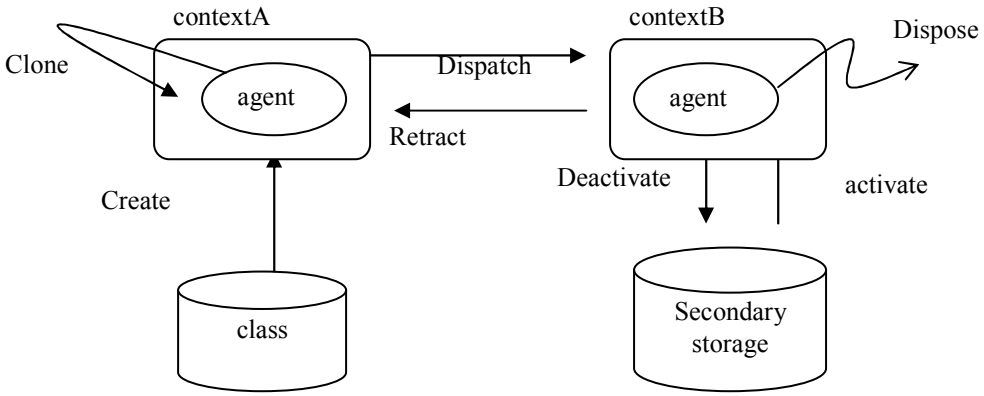

**Gambar 3**. Collaboration diagram detection agent

Untuk mewujudkan metode ini perlu dirancang komponen-komponen sistem keamanan jaringan berupa :
1. Intrusion detection system (IDS) Menggunakan agent bergerak (Aglets )
2. Database system
3. Monitoring system
4. Firewall system
5. SMS system




**Gambar 4** Arsitektur Sistem

Agent bergerak yang berfungsi sebagai sensor akan menangani pengumpulan data dan melaporkan hasil dari deteksi . Agent bergerak dapat melakukan operasi-operasi dasar seperti yang dijelaskan dibawah ini. Agent mempunyai kemampuan seperti digambarkan pada dibawah

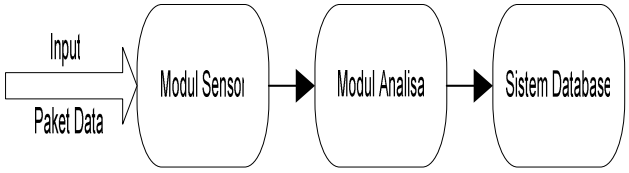



**Gambar 5** Model siklus hidup agent

1. *Creation:* penciptaan sebuah *agent*. *Creation* terjadi di dalam *context. Agent* yang baru diberi sebuah *identifier,* dimasukan ke dalam context dan diinisialisasi. *Aglet* mulai eksekusi segera setelah inisialisai sukses.
2. *Cloning:* proses penggandaan sebuah *agent. Cloning* menghasilkan turunan *(copy)* yang hampir identik dengan *aglet* yang asli didalam context yang sama.Perbedaannya hanya terletak pada *identifier* yang diberikan dan eksekusi aglet baru hasil cloning dimulai dari awal (*restart).* Catatan bahwa thread eksekusi tidak di -*clone* .
3. *Dispatching:* pemindahan sebuah *agent* dari satu *context* ke *context* yang lain. *Dispatching* akan memindahkan *agent* dari *context* yang sedang berlangsung, masuk ke *context* tujuan dan kemudian memulai awal eksekusinya.
4. *Retraction:* proses untuk "menarik" agent dari *context* yang sedang berlangsung dan masuk ke *context* yang melakukan permintaan retraction.
5. *Activation:* kemampuan untuk mengembalikan agent ke dalam *context.*
6. *Deactivation:* kemampuan untuk menghentikan sementara jalannya eksekusi aglet dan menyimpan state agent dalam penyimpan sekunder.
7. *Disposal:* proses untuk menghentikan jalannya eksekusi aglet yang sedang berlangsung dan mengeluarkan agent dari *context* yang sedang berlangsung.
8. *Messaging :* antar agent meliputi pengiriman, penerimaan dan penanganan message baik *synchronous* maupun *asynchronous.*

Intrusion Detection System (IDS) tediri dari komponen komponen :

1. Agent bergerak yang berfungsi sebagi sensor untuk mengumpulkan data
2. Analyzer
3. Database system




**Gambar 6.** Diagram Blok IDS

Agent bergerak , diatas disebutkan sebagai modul Sensor berfungsi untuk mengambil data dari jaringan. Sensor merupakan bagian dari sistem deteksi dini dari sistem keamanan yang dirancang. Untuk itu digunakan suatu program yang berfungsi sebagai *intrusion detector* dengan kemampuan packet logging dan analisis traffik yang realtime. *Analyzer* berfungsi untuk analisa paket yang lewat pada jaringan. Informasi dari analyzer yang akan menjadi input bagi sistem lainnya.

Perancangan Database untuk sistem keamanan jaringan

Sistem keamanan ini menggunakan prinsip sentralisasi database untuk menyimpan semua alert yang berasal dari sensor maupun log dari firewall.Informasi yang tersimpan pada data base ini juga merupakan input untuk pengawasan keamanan jaringan yang dilakukan oleh firewall system, monitoring system serta sistem notifikasi SMS. Database yang digunakan adalah MySQL yang diinstall pada sistem linux. Apabila database ini diinstall terpisah dari host firewall, bisa saja database ini diinstall pada sistem berbasis Windows atau sistem operasi lain yang mendukung database MySQL. Alasan pemilihan MySQL sebagai program database yang digunakan antara lain : Sifatnya yang open source dan murah Cukup stabil pada hardware dengan spesifikasi yang relatif rendahUntuk administrasi dan maintenance sistem database dibuat suatu interface berbasis web yang dibuat dengan bahasa pemrograman PHP. Fungsi utama dari interface ini adalah untuk mengedit atau mengupdate entry database yang dijadikan input bagi sistem yang lain.

Perancangan monitoring sistem

Sistem monitoring yang digunakan adalah sistem remote monitoring. Hal ini diperlukan karena dalam situasi yang umum monitoring sistem harus dapat dilakukan tanpa berada di lokasi host yang dipasang Untuk itu sistem monitoring yang paling fleksibel yang dapat diterapkan adalah sistem berbasis web. Untuk itu diperlukan sistem yang memiliki :

a. Linux kernel 2.4.xx
b. PHP
c. Web Server ( Apache )
d. Web Client ( pada sisi user )

Sistem remote monitoring yang akan digunakan, dirancang agar bersifat *user friendly*, sehingga masalah kemudahan pengguna dalam menggunakan *interface* ini bukan lagi menjadi masalah. Karena itu diterapkan sistem dengan *web interface.* Pemilihan *web interface* ini memiliki keunggulan sebagai berikut :

- Memudahkan network sistem administrator dalam menggunakan *interface*
- Pemakai tidak memerlukan keahlian linux dalam mengoperasikan *interface* ini
- Pada sisi *client* tidak memerlukan *software* tambahan, hanya memerlukan *browser* dan koneksi internet
- Kompatibel dengan berbagai macam *browser*

Analysis Console for Intrusion Databases ( ACID) merupakan *PHP-based analysis engine* yang berfungsi untuk mencari dan mengolah database dari alert network sekuriti yang dibangkitkan oleh perangkat lunak pendeteksi intrusi (IDS). Dapat di implementasikan pada sistem yang mendukung PHP seperti linux, BSD, Solaris dan OS lainnya. ACID adalah perangkat lunak yang open-source dan didistribusikan dibawah lisensi GPL. Pada tugas akhir ini digunakan ACID-0.9.6b23 dan PHP 4.3.3

ACID mempunyai kemampuan :

- **Query-builder and search interface** untuk mencari alert yang sesuai dengan Alert meta information (seperti : *signature, detection time*) juga data data network (seperti : *source / destination address, ports, payload* atau *flags*).

- **Packet viewer (decoder)** untuk mendisplay grafik informasi alert layer 3 (Transport :TCP, UDP ) dan layer 4 ( Network : IP, IPX )

- **Alert management** ( manajemen peringatan ) berfungsi untuk membuat grup alert, membuang alert yang dianggap semu atau palsu, mengirimkan alert ke email serta mendukung pengarsipan alert agar dapat dipindahkan antar database alert.

- **Chart and statistics generation** membuat chart dan statistic berdasar pada waktu, sensor, signature, protokol, IP address, TCP/UDP ports, klasifikasi.

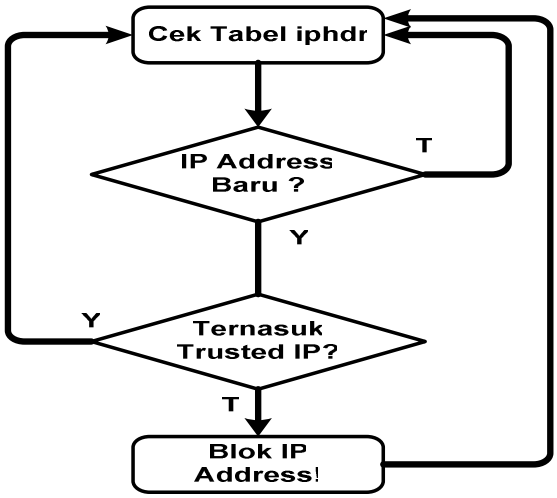
ACID merupakan aplikasi web based, sehingga semua informasi informasi keadaan kemanan jaringan berupa alert dari sensor dan log dari firewall dapat dianalisa melalui aplikasi web browser (seperti : Mozilla, Konqueror, Opera). Informasi ini akan menjadi bahan untuk *security audit. Security auidit* perlu dilakukan agar kemanan jaringan tetap terjamin dan untuk mendapatkan solusi keamanan jaringan yang lebih baik

Untuk itu diperlukan pengkonfigurasian pada HTTP server ( Apache ) yang sudah terinstall pada host. HTTP server yang terinstal adalah Apache server 1.3.28. Apabila diinginkan fitur enkripsi pada informasi yang dikirimkan sistem monitoring pada browser, dapat ditambahkan modul SSL pada web server tersebut. Hal ini akan meningkatkan keamanan data yang dikirimkan monitoring system pada administrator dari kemungkinan penyadapan data ( man-in-the-middle attack ).

ACID berfungsi menyediakan management console yang dapat diakses melalui web browser. Fungsi *managemenet console* ini adalah sebagai interface untuk network system administrator (NSA) agar dapat melakukan observasi pada kebijaksanaan keamanan

Perancangan Firewall

Program firewall otomatis yang dibuat pada dasarnya adalah program yang menganalisa output dari Intrusion Detection System (IDS) serta memutuskan tindakan yang harus diambil untuk host pengirim paket yang dianalisa tersebut. Apabila paket tersebut oleh IDS dikategorikan sebagai paket berbahaya atau mengandung resiko keamanan jaringan, maka program firewall otomatis akan memicu program iptables untuk menambahkan sebuah rule yang memblok semua paket yang berasal dari host paket yang mencurigakan tersebut. Berikut Flow chart dari sistem firewall otomatis.

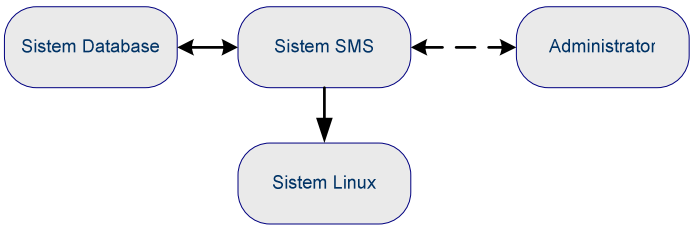



**Gambar 7**. Flowchart proses firewall

Perancangan sistem notifikasi SMS

Sistem notifikasi SMS ini dirancang sebagai bagian yang memberikan fungsi interaktif antara sistem dengan administrator. Alasan digunakannya SMS sebagai media interaktif adalah sebagai berikut :

- Penyampaian pesan yang cepat dan cukup reliable
- Biaya yang relatif murah
- Bersifat dua arah
- Tidak tergantung pada jaringan data host




**Gambar 8**. Diagram Blok Interkoneksi Sistem Notifikasi SMS (

Fungsi dasar dari sistem SMS ini sebenarnya hanya memberikan notifikasi atau pemberitahuan kepada administrator sesegera mungkin ketika terjadi suatu event yang mentrigger firewall untuk memblok IP address suatu host dan di-log dalam database. Proses insertion dalam database inilah yang mentrigger sistem SMS untuk mengirimkan pesan SMS kepada administrator. Pesan yang dikirimkan berisi tentang IP address dari host yang diblok oleh sistem.

Perlu diperhatikan bahwa fungsi dasar sistem SMS ini tidak melakukan interupsi apapun pada proses perlindungan sistem oleh AIRIDS. Karena yang dilakukan oleh sistem SMS hanyalah mengecek tabel yang berisi daftar IP address yang sudah diblok secara periodik. Oleh karena itu jika hanya fungsi dasar ini yang dibutuhkan, maka sistem SMS dapat dipasang dimana saja, sejauh masih bisa mengakses database yang digunakan oleh AIRIDS.

Tetapi untuk mendapatkan interaktivitas penuh dari sistem SMS ini, maka sistem SMS harus dipasang pada host yang dipasangi AIRIDS. Hal ini diperlukan karena interaktivitas penuh dari sistem SMS ini memerlukan akses pada sistem untuk mengeksekusi berbagi perintah yang diberikan oleh administrator melalui SMS.

Manfaat penerapan sistem SMS dengan interaktivitas penuh antara lain :

- Dapat mengembalikan kondisi sistem apabila blocking IP address yang terjadi adalah karena kekeliruan admin saat melakukan administrasi atau testing pada host secara remote.
- Dapat mengakses sistem secara remote bahkan ketika jaringan down meskipun secara terbatas.
- Dapat mengeksekusi emergency command sesegera mungkin untuk menyelamatkan data atau sistem. Misal dengan mengembalikan password root atau bahkan me-*reboot* atau meng-*halt* sistem.

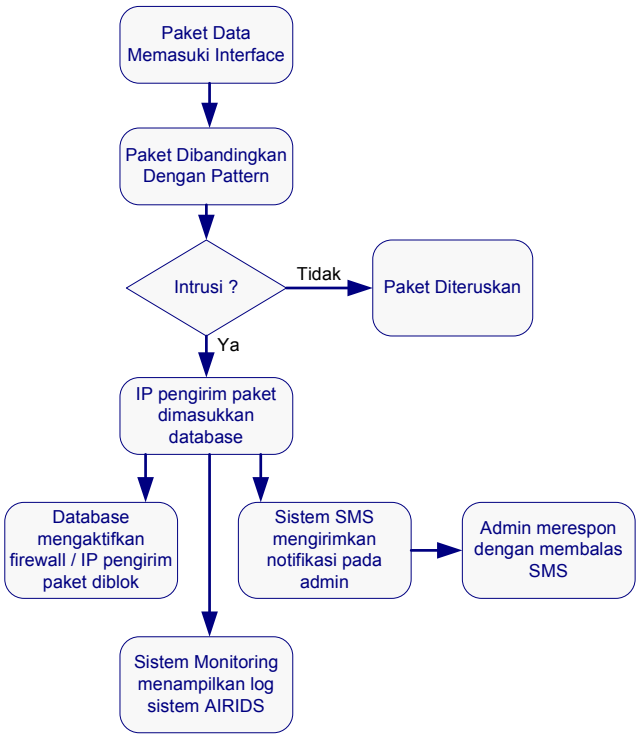
Pada fungsi normalnya, program sistem SMS akan mengakses database AIRIDS untuk mengecek kondisi tabel blocking IP address serta untuk mengambil sintaks perintah sistem yang harus dieksekusi sebagai respon admin pada suatu kondisi tertentu. Hal ini menimbulkan satu kelemahan yaitu ketergantungan sistem SMS pada database. Apabila database down, maka sistem SMS tidak akan dapat berfungsi sama sekali.

Hal ini diatasi dengan membuat prosedur *emergency* atau darurat pada program sistem SMS. Prosedur ini berguna untuk menjaga ketersediaan akses admin pada sistem melalui SMS walaupun database tidak berfungsi. Pada implementasinya, program dirancang untuk dapat mengeksekusi perintah berupa *full syntax* yang dikirimkan admin melalui SMS. Selain itu, untuk mempermudah, singakatan dari berbagai sintaks dapat langsung dimasukkan dalam source code program SMS atau diambil dari file lain dalam sistem.

Perancangan Sistem Terintegrasi Serta Interaksinya Dengan User

Keseluruhan sistem diatas diintegrasikan dalam sebuah sistem yang dibangun pada platform yang disesuaikan dengan kondisi sistem yang ada, baik itu sistem operasi, konfigurasi jaringan maupun policy jaringan yang telah ditentukan. Diagram interkoneksi antar sistem pembangun dapat dilihat kembali pada gambar berikut ini :

Flowchart proses program serta interaksinya dengan user sebagai berikut :




**Gambar 9.** Flowchart Proses Sistem

Sistem terintegrasi ini dirancang agar dapat dieksekusi secara tunggal dengan tujuan agar program-program dalam masing-masing sistem dapat berjalan secara sinkron. Alasan lainnya adalah untuk kemudahan pengguna. Oleh karena itu eksekusi program-program sistem pendukung dimasukkan dalam program firewall otomatis. Administrator sistem sebagai pengguna dapat berhubungan dengan sistem AIRIDS ini melalui sistem monitoring ACID secara satu arah ataupun melalui sistem notifikasi SMS secara dua arah.

Desain sistem seperti di atas memberikan administrator sistem fleksibilitas dalam me-maintain sistemnya. Sehingga efisiensi kerja dari administrator semakin baik sekaligus meningkatkan keandalan sistem dalam menghadapi resiko keamanan dari jaringan. Kekurangan yang jelas timbul dari adanya sistem ini adalah delay yang timbul dalam proses forwarding paket. Oleh karena itu sistem ini harus diimplementasikan sedemikian rupa sehingga memiliki efisiensi yang tinggi baik dalam algoritma maupun penggunaan resource yang ada pada sistem.

## 5. KESIMPULAN

Telah berhasil dibuat arsitektur *intrusion detection system* menggunakan pendekatan agent bergerak sebagai pengganti sensor untuk menentukan penyusupan.

## 6. DAFTAR PUSTAKA

Bursell , M., 2009, *A Aglets Puppies Workshop*, online pada www.ansa.co.uk/ANSATech/FollowMe/**Puppies**/apm/**workshop**/**AGLETS**.pdf. 27 Februari 2009.

Bace, R., dan Mell, P., 2002, "Intrusion Detection System": NIST Special Publication On IDS, online pada http://www.snort.org/docs/nist-ids.pdf , 25 Februari 2009

Balasubramaniyan, J.S., Fernandes, J.O.G., Isacoff, D., Spaffoer, E,. and Zamboni, D., 1998, "An Architecture For Intrusion Detection Using Autonomous Agents" ,online pada https://www.cerias.purdue.edu/assets/pdf/bibtex_archive/98-05.pdf. 27 Februari 2009.

Dune, C.R., 2000, "Using Mobile Agents For Network Resource Discovery In PeerToPeerNetworks",onlinepadahttp://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.98.4772. 27 Februari 2009

Firrar U., Riyanto B, 2003, Design dan Implementasi Mobile Agent Untuk Jaringan, Thesis ITB

Farmer, D., dan Venema, W., 2009, *Improving The Security of Your Site by Breaking in to it*,online pada http://www.porcupine.org/satan/admin-guide-to-cracking.html. 27 Februari 2009.

Gunawan Adi S, 2003 , Design dan implementasi Sistem Deteksi Penyusupan Jaringan Secara Otomatis dan Interaktif , ITB

Gopalakrishna, R., dan Spafford, E., 2000, "A Framework for distributed Intrusion Detection Using Interest Driven Cooperative Agents", online pada http://www.raid-symposium.org/Raid2001/papers/gopalakrishna_spafford_raid2001.pdf. 24 Februari 2009.

Hidayat, S,S.,2002, "Notifikasi dan Akses Database Terdistribusi Menggunakan Agent", Thesis Institut Teknologi Bandung.

Hunt, C., 1992, *TCP/IP Network Administration,* O'Reilly & Associates, Inc

Is,. 2009, *A Strategy for a Successful IDS Evaluation, Atlanta*: Internet Security Systems, online pada www.enterprisesecuritysolutions.**net**/files/**IDS**_presentation.ppt.29 Februari 2009

Firrar U,. Riyanto B, 2003, Design dan implementasi Mobile Agent ,Thesis magister ITB

Gunawan Adi S, 2003, Design dan implementasi Sistem deteksi penyusupan secara otomatis dan interaktif, ITB